日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年　３月３１日

出 願 番 号
Application Number: 特願２００３－０９６２４０

[ST. 10/C]: ［ＪＰ２００３－０９６２４０］

出 願 人
Applicant(s): 株式会社リコー

２００３年１０月２９日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８９６２１

【書類名】　特許願
【整理番号】　0302583
【提出日】　平成15年 3月31日
【あて先】　特許庁長官　殿
【国際特許分類】　G03G 21/00　396
【発明の名称】　情報処理装置とその情報管理システムおよびデジタル証明書取得方法並びにプログラム
【請求項の数】　21
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
【氏名】　小椋　正明
【特許出願人】
【識別番号】　000006747
【住所又は居所】　東京都大田区中馬込１丁目３番６号
【氏名又は名称】　株式会社リコー
【代表者】　桜井　正光
【代理人】
【識別番号】　100080931
【住所又は居所】　東京都豊島区東池袋１丁目２０番２号　池袋ホワイトハウスビル８１８号
【弁理士】
【氏名又は名称】　大澤　敬
【手数料の表示】
【予納台帳番号】　014498
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【包括委任状番号】　9809113

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報処理装置とその情報管理システムおよびデジタル証明書取得方法並びにプログラム

【特許請求の範囲】

【請求項１】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知し、その識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置から該識別情報を含むデジタル証明書を受信した場合に、そのデジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項２】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、前記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項３】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受

信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項４】　請求項２又は３記載のデジタル証明書取得方法において、

当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化することを特徴とするデジタル証明書取得方法。

【請求項５】　請求項２乃至４のいずれか一項に記載のデジタル証明書取得方法において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定することを特徴とするデジタル証明書取得方法。

【請求項６】　請求項２乃至４のいずれか一項に記載のデジタル証明書取得方法において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除することを特徴とするデジタル証明書取得方法。

【請求項７】　通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴

とする情報処理装置。

【請求項８】　通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

情報を入力する入力手段と、

情報を記憶する記憶手段と、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、

該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、

前記生産台数分の通信装置の識別情報のいずれかが前記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴とする情報処理装置。

【請求項９】　通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

バーコードを読み取る読取手段と、

情報を記憶する記憶手段と、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、

該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、

前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、

そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴とする情報処理装置。

【請求項１０】　請求項８又は９記載の情報処理装置において、

前記デジタル証明書送信手段は、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を有することを特徴とする情報処理装置。

【請求項１１】　請求項８乃至１０のいずれか一項に記載の情報処理装置において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたことを特徴とする情報処理装置。

【請求項１２】　請求項８乃至１０のいずれか一項に記載の情報処理装置において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたことを特徴とする情報処理装置。

【請求項１３】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された識別情報を含むデジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成されたデジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項１４】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、情報を入力する入力手段と、情報を記憶する記憶手段と、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、前記生産台数分の通信装置の識別情報のいずれかが前記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項１５】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に

該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項１６】　請求項１４又は１５記載の情報管理システムにおいて、

前記情報処理装置のデジタル証明書送信手段は、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を有することを特徴とする情報管理システム。

【請求項１７】　請求項１４乃至１６のいずれか一項に記載の情報管理システムにおいて、

前記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたことを特徴とする情報管理システム。

【請求項１８】　請求項１４乃至１６のいずれか一項に記載の情報管理システムにおいて、

前記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から

削除するデジタル証明書削除手段を設けたことを特徴とする情報管理システム。

【請求項１９】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【請求項２０】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、前記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【請求項２１】　通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、前記生産台数分の通信装置のいずれ

かに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を前記デジタル証明書保存手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、この情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システム、および上記情報処理装置におけるデジタル証明書取得方法、並びに上記情報処理装置を制御するコンピュータに必要な機能（この発明に係わる機能）を実現させるためのプログラムに関する。

【０００２】

【従来の技術】

従来から、通信機能を備えたプリンタ，ファクシミリ（ＦＡＸ）装置，デジタル複写機，スキャナ装置，デジタル複合機等の画像処理装置を始め、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム等に通信機能（通信手段）を持たせた通信装置（電子装置）を被管理装置とし、サービスセンタ（管理センタ）の中央管理装置が公衆回線やインタネット等のネットワーク経由でこれらの被管理装置を遠隔管理する遠隔管理システムが提案されている。

【０００３】

あるいは、被管理装置が通信機能を備えていない場合や、通信機能を備えていてもその機能が中央管理装置と通信するための機能を持っていない場合には、その被管理装置に中央管理装置と通信可能な通信機能を有する仲介装置をネットワーク経由で接続し、中央管理装置がネットワークおよび仲介装置経由で被管理装置を遠隔管理する遠隔管理システムも提案されている。

【０００４】

一方、従来から、ＰＣ（パーソナルコンピュータ）等のコンピュータを複数台ネットワークを介して通信可能に接続し、少なくとも１台をサーバ装置（サーバ）、別の少なくとも１台をクライアント装置（クライアント）としたクライアント・サーバシステムを構成することが行われている。

このようなクライアント・サーバシステムにおいては、クライアント装置からサーバ装置に要求を送信し、サーバ装置がその要求に従った処理を行ってクライアント装置に対して応答を返す。

【０００５】

したがって、上述した遠隔管理システムにおいて、通信装置あるいは通信装置が接続された仲介装置にクライアント装置の機能を、中央管理装置にサーバ装置の機能をそれぞれ持たせ、通信装置又は仲介装置をファイアウォールおよびネットワーク経由で中央管理装置と接続した場合には、通信装置又は仲介装置がポーリング（送信要求があるかどうかの問い合わせ）を中央管理装置に通知し、その中央管理装置がそのポーリングに従った処理を行って通信装置又は仲介装置に対して応答を返すことができる。

例えば、中央管理装置は、仲介装置からポーリングを受けると、課金カウンタ取得要求をその仲介装置へ通知する。

【０００６】

ポーリング通知元の仲介装置は、中央管理装置から課金カウンタ取得要求を受けると、その課金カウンタ取得要求を自己に接続されている画像形成装置へ通知する。

その画像形成装置は、仲介装置から課金カウンタ取得要求を受けると、不揮発性メモリに格納されている課金カウンタのデータを読み取り、その読み取った課金カウンタのデータ（応答データ）を仲介装置へ送信する。

仲介装置は、画像形成装置から課金カウンタのデータを受信すると、それを中央管理装置へ送信する。

【０００７】

このような場合においては、通信相手が適切か、あるいは送信される情報が改

ざんされていないかといった確認が重要である。また、特にインターネットにおいては、情報が通信相手に到達するまでに無関係なコンピュータを経由する場合が多いことから、機密データ（課金カウンタのデータ等）を送信する場合、その内容を盗み見られないようにする必要もある。そして、このような要求に応える通信プロトコルとして、例えばＳＳＬ（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、データの暗号化により改ざんおよび盗聴の防止を図ることができる。

【０００８】

ここで、このＳＳＬを用いて相互認証を行う場合の通信手順について、認証処理の部分に焦点を当てて説明する。

図２４は、クライアント装置（通信装置又は仲介装置）とサーバ装置（仲介装置）とがＳＳＬによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

図２４に示すように、ＳＳＬによる相互認証を行う際には、まずクライアント装置側にルート鍵証明書，クライアント私有鍵，クライアント公開鍵証明書（クライアント証明書）を記憶させておく必要がある。クライアント私有鍵は、認証局（ＣＡ：certificate authority）がクライアント装置に対して発行した私有鍵である。そして、クライアント公開鍵証明書は、その私有鍵と対応する公開鍵にＣＡがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、ＣＡがデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。

【０００９】

図２５にこれらの関係を示す。

図２５（ａ）に示すように、クライアント公開鍵は、クライアント私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（ＣＡ），発行相手（クライアント装置），有効期限等の情報を含む書誌情報とによっ

て構成される。そして、ＣＡは、鍵本体や書誌情報が改竄されていないことを示すため、クライアント公開鍵をハッシュ処理して得たハッシュ値を、ルート私有鍵を用いて暗号化し、デジタル署名としてクライアント公開鍵に付す。またこの際に、デジタル署名に用いるルート私有鍵の識別情報を署名鍵情報として公開鍵の書誌情報に加える。そして、このデジタル署名を付した公開鍵証明書が、クライアント公開鍵証明書である。

【００１０】

このクライアント公開鍵証明書を認証処理に用いる場合には、ここに含まれるデジタル署名を、ルート私有鍵と対応する公開鍵であるルート鍵の鍵本体を用いて復号化する。この復号化が正常に行われれば、デジタル署名が確かにＣＡによって付されたことがわかる。また、クライアント公開鍵部分をハッシュ処理して得たハッシュ値と、復号して得たハッシュ値とが一致すれば、鍵自体も損傷や改竄を受けていないことがわかる。さらに、受信したデータをこのクライアント公開鍵を用いて正常に復号化できれば、そのデータは、クライアント私有鍵の持ち主、つまりクライアント装置から送信されたものであることがわかる。あとは、書誌情報を参照して、ＣＡの信頼性やクライアント装置の登録有無等によって認証の正否を決定すればよい。

【００１１】

ここで、認証を行うためには、ルート鍵を予め記憶しておく必要があるが、このルート鍵も、図２５（ｂ）に示すように、ＣＡがデジタル署名を付したルート鍵証明書として記憶しておく。このルート鍵証明書は、自身に含まれる公開鍵でデジタル署名を復号化可能な、自己署名形式である。そして、ルート鍵を使用する際に、そのルート鍵証明書に含まれる鍵本体を用いてデジタル署名を復号化し、ルート鍵をハッシュ処理して得たハッシュ値と比較する。これが一致すれば、ルート鍵が破損等していないことを確認できるのである。

【００１２】

図２４の説明に戻ると、サーバ装置側には、ルート鍵証明書，サーバ私有鍵，サーバ公開鍵証明書（サーバ証明書）を記憶させておく必要がある。サーバ私有鍵及びサーバ公開鍵証明書は、ＣＡがサーバ装置に対して発行した私有鍵及び公

開鍵証明書である。ここではクライアント装置とサーバ装置に対して同じＣＡが同じルート私有鍵を用いて証明書を発行しているものとし、この場合にはルート鍵証明書はクライアント装置とサーバ装置で共通となる。

【００１３】

フローチャートの説明に入る。なお、図２４において、２本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。

【００１４】

クライアント・サーバシステムにおいて、接続を要求するのはクライアント装置側であるが、ユーザの指示等によってこの必要が生じた場合、クライアント装置のＣＰＵは、所要の制御プログラムを実行することにより、図２４の左側に示すフローチャートの処理を開始する。そして、ステップＳ１１でサーバ装置に対して接続要求を送信する。

一方サーバ装置のＣＰＵは、この接続要求を受信すると、所要の制御プログラムを実行することにより、図２４の右側に示すフローチャートの処理を開始する。そして、ステップＳ２１で第１の乱数を生成し、これをサーバ私有鍵を用いて暗号化する。そして、ステップＳ２２でその暗号化した第１の乱数とサーバ公開鍵証明書とをクライアント装置に送信する。このステップＳ２２の処理において、サーバ装置のＣＰＵが第１のサーバ側認証処理手段として機能する。

【００１５】

クライアント装置側では、これを受信すると、ステップＳ１２でルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認する。これには、上述のように損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップＳ１３で、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて第１の乱数を復号化する。ここで復号化が成功すれ

ば、第１の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置から受信したものだと確認できる。そして、サーバ装置を正当な通信相手として認証する。このステップＳ１２及びＳ１３の処理において、クライアント装置のＣＰＵが第２のクライアント側認証処理手段として機能する。

【００１６】

その後、ステップＳ１４でこれとは別に第２の乱数及び第３の乱数を生成する。そして、ステップＳ１５で第２の乱数をクライアント私有鍵を用いて暗号化し、第３の乱数をサーバ公開鍵を用いて暗号化し、ステップＳ１６でこれらをクライアント公開鍵証明書と共にサーバ装置に送信する。第３の乱数の暗号化は、サーバ装置以外の装置に乱数を知られないようにするために行うものである。このステップＳ１６の処理において、クライアント装置のＣＰＵが第１のクライアント側認証処理手段として機能する。

【００１７】

サーバ装置側では、これを受信すると、ステップＳ２３でルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認する。これにも、ステップＳ１２の場合と同様、クライアント装置が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップＳ２４で、受信したクライアント公開鍵証明書に含まれるクライアント公開鍵を用いて第２の乱数を復号化する。ここで復号化が成功すれば、第２の乱数は確かにクライアント公開鍵証明書の発行対象であるクライアント装置から受信したものだと確認できる。そして、サーバ装置を正当な通信相手として認証する。このステップＳ２３及び２４の処理において、サーバ装置のＣＰＵが第２のサーバ側認証処理手段として機能する。

【００１８】

その後、ステップＳ２５でサーバ私有鍵を用いて第３の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第１乃至第３の乱数が共有されたことになる。そして、少なくとも第３の乱数は、生成したクライアント装置と、サーバ私有鍵を持つサーバ装置以外の装置が知ることはない。ここまでの処理が成功すると、ステップＳ２６でクライアント装置に対して認証成功の応答を返す。

【００１９】

クライアント装置側では、これを受信すると、ステップＳ１７で第１乃至第３の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。サーバ装置側でも、ステップＳ２７で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップＳ１７又はＳ２７で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

このような処理を行うことにより、クライアント装置とサーバ装置が互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。

【００２０】

ところで、上述した遠隔管理システムにおいても、通信装置が、中央管理装置とＳＳＬによる相互認証を行って通信可能にするためには、内部メモリ（記憶手段）にデジタル証明書（ルート鍵証明書，クライアント私有鍵，クライアント公開鍵証明書）を予め記憶（保存）させておく必要がある。デジタル証明書は、ＣＡ（認証局）から取得することができる。その取得に関しては、例えば特許文献１に記載されている。また、通信装置の販売会社と保守契約をする必要があり、それによって中央管理装置による遠隔管理が可能になる。

【００２１】

【特許文献１】

特開２００１－３２５２４９号公報

【００２２】

【発明が解決しようとする課題】

遠隔管理システムに使用される通信装置は、毎日、機種毎に決定された台数分だけ生産されるようになっており、その機種毎に内部メモリにデジタル証明書を記憶させるかどうか、つまり中央管理装置による遠隔管理に対応できるかどうかも決定される。注文生産されるものではないため、保守契約後、内部メモリにデジタル証明書を記憶した通信装置を生産する、ということはできない。

よって、機種によっては、保守契約をしていなくても、内部メモリにデジタル

証明書を記憶した通信装置は当然存在するため、その通信装置を保守契約した通信装置とし、管理装置によって遠隔管理されるようにすることも可能である。

【００２３】

例えば、２台の通信装置を所有する機器利用者が、保守契約している通信装置の課金カウンタの値より保守契約していない通信装置の課金カウンタの値が小さいような場合、後者の通信装置の方が保守料金が安く済むため、その通信装置を前者の通信装置とし、課金カウンタの値を示すカウンタ情報を中央管理装置へ送信することも可能である。その場合、中央管理装置側では、後者の通信装置から受信したカウンタ情報に基づいて保守料金を計算するため、その保守料金、つまり安い方の保守料金を機器利用者に請求することになる。

【００２４】

この発明は、上記の問題点に鑑みてなされたものであり、中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定できるようにすることを目的とする。

【００２５】

【課題を解決するための手段】

この発明は、上記の目的を達成するため、情報処理装置、情報管理システム、および上記情報処理装置におけるデジタル証明書取得方法、並びに上記情報処理装置を制御するコンピュータに必要な機能を実現させるためのプログラムを提供する。

【００２６】

請求項１の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知し、その識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置から該識別情報を含むデジタル証明書を受信した場合に、そのデジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【００２７】

請求項２の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、上記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【００２８】

請求項３の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【００２９】

請求項４の発明によるデジタル証明書取得方法は、請求項２又は３のデジタル証明書取得方法において、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書

を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化するものである。

請求項５の発明によるデジタル証明書取得方法は、請求項２～４のいずれかのデジタル証明書取得方法において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定するものである。

請求項６の発明によるデジタル証明書取得方法は、請求項２～４のいずれかのデジタル証明書取得方法において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するものである。

【００３０】

請求項７の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【００３１】

請求項８の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、情報を入力する入力手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置の識別情報のいずれかが上記

入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【００３２】

請求項９の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【００３３】

請求項１０の発明による情報処理装置は、請求項８又は９の情報処理装置において、上記デジタル証明書送信手段に、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を備えたものである。

請求項１１の発明による情報処理装置は、請求項８～１０のいずれかの情報処理装置において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたものである。

請求項１２の発明による情報処理装置は、請求項８～１０のいずれかの情報処

理装置において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたものである。

【００３４】

請求項１３の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された識別情報を含むデジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成されたデジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【００３５】

請求項１４の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、情報を入力する入力手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と

、上記生産台数分の通信装置の識別情報のいずれかが上記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【００３６】

請求項１５の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【００３７】

請求項１６の発明による情報管理システムは、請求項１４又は１５の情報管理システムにおいて、上記情報処理装置のデジタル証明書送信手段に、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を備えたものである。

請求項１７の発明による情報管理システムは、請求項１４～１６のいずれかの情報管理システムにおいて、上記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたものである。

請求項１８の発明による情報管理システムは、請求項１４～１６のいずれかの情報管理システムにおいて、上記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたものである。

【００３８】

請求項１９の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【００３９】

請求項２０の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の

識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、上記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【００４０】

請求項２１の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を上記デジタル証明書保存手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【００４１】

【発明の実施の形態】

以下、この発明の好ましい実施の形態を図面を参照して説明する。

まず、この発明による通信装置を被管理装置とする遠隔管理システムの構成例について説明する。図１は、その遠隔管理システムの構成の一例を示す概念図で

ある。

【００４２】

この遠隔管理システムは、プリンタ，ＦＡＸ装置，デジタル複写機，スキャナ装置，デジタル複合機等の画像処理装置や、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム等に通信機能を持たせた通信装置（電子装置）を被管理装置１０（１０ａ，１０ｂ，１０ｃ，１０ｄ，１０ｅ，１０ｆ）とする遠隔管理システムである。そして、この被管理装置１０と接続される（被管理装置側から見た）外部装置として、被管理装置１０とＬＡＮ（ローカルエリアネットワーク）によって接続された遠隔管理仲介装置である仲介装置１０１（１０１ａ，１０１ｂ，１０１ｃ）、更に仲介装置１０１とインタネット１０３（公衆回線等の他のネットワークでもよい）を介して接続されるサーバ装置として機能する中央管理装置（以下単に「管理装置」ともいう）１０２を備え、当該中央管理装置１０２が、仲介装置１０１を介して各被管理装置１０を集中的に遠隔管理できるようにしたものである。当該仲介装置１０１および被管理装置１０は、その利用環境に応じて多様な階層構造を成す。

【００４３】

例えば、図１に示す設置環境Ａでは、中央管理装置１０２とＨＴＴＰ（Hyper Text Transfer Protocol）による直接的なコネクションを確立できる仲介装置１０１ａが、被管理装置１０ａ及び１０ｂを従える単純な階層構造になっているが、同図に示す設置環境Ｂでは、４台の被管理装置１０を設置するため、１台の仲介装置１０１を設置しただけでは負荷が大きくなる。そのため、中央管理装置１０２とＨＴＴＰによる直接的なコネクションを確立できる仲介装置１０１ｂが、被管理装置１０ｃおよび１０ｄだけでなく、他の仲介装置１０１ｃを従え、この仲介装置１０１ｃが被管理装置１０ｅおよび１０ｆを更に従えるという階層構造を形成している。この場合、被管理装置１０ｅおよび１０ｆを遠隔管理するために中央管理装置１０２から発せられた情報は、仲介装置１０１ｂとその下位のノードである仲介装置１０１ｃとを経由して、被管理装置１０ｅ又は１０ｆに到達することになる。

【００４４】

また、設置環境Ｃのように、被管理装置１０に仲介装置１０１の機能を併せ持たせた仲介機能付被管理装置（以下単に「被管理装置」ともいう）１１ａ，１１ｂを、別途仲介装置を介さずにインタネット１０３によって中央管理装置１０２に接続するようにしてもよい。

図示はしていないが、仲介機能付被管理装置１１の下位に更に被管理装置１０と同等の被管理装置を接続することもできる。

なお、各設置環境Ａ，Ｂ，Ｃには、セキュリティ面を考慮し、ファイアウォール１０４を設置する。

また、この遠隔管理システムにおいては、サービスセンタＳの中央管理装置１０２に、後述する生産工場Ｅの通信端末１５０が接続されている。

【００４５】

このような遠隔管理システムにおいて、仲介装置１０１は、これに接続された被管理装置１０の制御管理のためのアプリケーションプログラムを実装している。

中央管理装置１０２は、各仲介装置１０１の制御管理、更にはこの仲介装置１０１を介した被管理装置１０の制御管理を行うためのアプリケーションプログラムを実装している。そして、被管理装置１０も含め、この遠隔管理システムにおけるこれら各ノードは、ＲＰＣ（remote procedure call）により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【００４６】

すなわち、仲介装置１０１又はこれと接続された被管理装置１０では、中央管理装置１０２への要求を生成してこれを中央管理装置１０２へ引き渡し、この要求に対する応答を取得できる一方で、中央管理装置１０２は、上記仲介装置１０１側への要求を生成してこれを仲介装置１０１側へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、仲介装置１０１に被管理装置１０に対して各種要求を送信させ、被管理装置１０からの応答を仲介装置１０１を介して取得することも含まれる。

なお、ＲＰＣを実現するために、ＳＯＡＰ（Simple Object Access Protocol），ＨＴＴＰ，ＦＴＰ（File Transfer Protocol），ＣＯＭ（Component Object Model），ＣＯＲＢＡ（Common Object Request Broker Architecture）等の既知のプロトコル（通信規格），技術，仕様などを利用することができる。

【００４７】

この送受信のデータ送受モデルを図２の概念図に示す。

（Ａ）は、被管理装置１０で中央管理装置１０２に対する要求が発生したケースである。このケースでは、被管理装置１０が被管理装置側要求ａを生成し、これを仲介装置１０１を経由して受け取った中央管理装置１０２がこの要求に対する応答ａを返すというモデルになる。同図に示す仲介装置１０１は複数であるケースも想定できる（上記図１に示す設置環境Ｂ）。なお、（Ａ）では、応答ａだけでなく応答遅延通知ａ´を返信するケースが表記されている。これは、中央管理装置１０２を、仲介装置１０１を経由して被管理装置側要求を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次回の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

【００４８】

（Ｂ）は、中央管理装置１０２で被管理装置１０に対する要求が発生したケースである。このケースでは、中央管理装置１０２が管理装置側要求ｂを生成し、これを仲介装置１０１を経由して受け取った被管理装置１０が、当該要求に対する応答ｂを返すというモデルになっている。なお、（Ｂ）のケースでも、応答を即座に返せないときに応答遅延通知ｂ´を返すことは（Ａ）のケースと同様である。

【００４９】

次に、図１に示す中央管理装置１０２の物理的構成について簡単に説明すると、当該中央管理装置１０２は、ＣＰＵ，ＲＯＭ，ＲＡＭ等からなる制御装置や、データベース，モデム，プロシキサーバ等によって構成されている。その構成については、追って詳細に説明する。

さらに、図１に示す仲介装置１０１の物理的構成について説明すると、当該仲

介装置１０１は、不図示のＣＰＵ，ＲＯＭ，ＲＡＭ，不揮発性メモリ，ネットワークインタフェースカード（ＮＩＣ）等によって構成されている。

また、仲介機能付被管理装置１１については、仲介装置１０１の機能を実現するためにこれらのユニットを単に被管理装置１０に付加しても良いが、被管理装置１０に備えるＣＰＵ，ＲＯＭ，ＲＡＭ等のハードウェア資源を利用し、ＣＰＵに適当なアプリケーションやプログラムモジュールを実行させることによって仲介装置１０１の機能を実現することもできる。

【００５０】

以下、図１に示した遠隔管理システムのより具体的な例として、この発明による通信装置である画像形成装置を被管理装置とした、この発明による通信装置の遠隔管理システムである画像形成装置遠隔管理システムについて説明する。図３は、その画像形成装置遠隔管理システムの構成の一例を示す概念図であるが、被管理装置１０を画像形成装置１００に、仲介機能付被管理装置１１を仲介機能付画像形成装置（以下単に「画像形成装置」ともいう）１１０に変更した点が図１と相違するのみであるので、システムの全体構成についての説明は省略する。

画像形成装置１００は、コピー，ファクシミリ，スキャナ等の機能および外部装置と通信を行う機能を備えたデジタル複合機であり、それらの機能に係るサービスを提供するためのアプリケーションプログラムを実装しているものである。また、仲介機能付画像形成装置１１０は、画像形成装置１００に仲介装置１０１の機能を併せ持たせたものである。

【００５１】

このような画像形成装置１００の物理的構成について図４を用いて説明する。

図４は、画像形成装置１００内のハードウェア構成例を示すブロック図である。図５はフラッシュメモリ２０４の記憶エリアの構成例を、図６はＮＶＲＡＭ２０７の記憶エリアの構成例をそれぞれ示すメモリマップ図である。

この画像形成装置１００は、ＣＰＵ２０１，ＡＳＩＣ（Application Specific Integrated Circuit）２０２，ＳＤＲＡＭ２０３，フラッシュメモリ（不揮発性メモリ）２０４，ＮＲＳ用メモリ２０５，ＰＨＹ（物理メディアインタフェース）２０６，ＮＶ－ＲＡＭ（不揮発性メモリ）２０７，操作部２０９，ＨＤＤ（

ハードディスクドライブ）２１０，モデム２１１，ＰＩ（パーソナルインタフェース）２１２，ＦＣＵ（ファックスコントロールユニット）２１３，ＵＳＢ（Universal Serial Bus）２１４，ＩＥＥＥ１３９４２１５，ＬＰ（読み取り・書き込み部）２１６，および周辺機２１７を備えている。

【００５２】

ＣＰＵ２０１は、ＡＳＩＣ２０２を介してデータ処理（各機能の制御）を行う演算処理手段である。

ＡＳＩＣ２０２は、ＣＰＵインターフェース，ＳＤＲＡＭインターフェース，ローカルバスインタフェース，ＰＣＩインタフェース，ＭＡＣ（Media Access Controller）、ＨＤＤインタフェースなどからなる多機能デバイスボードであり、ＣＰＵ２０１の制御対象となるデバイスの共有化を図り、アーキテクチャの面からアプリ（アプリケーションソフト）や共通システムサービスの開発の高効率化を支援するものである。

ＳＤＲＡＭ２０３は、ＯＳを含む各種プログラムを記憶するプログラムメモリや、ＣＰＵ２０１がデータ処理を行う際に使用するワークメモリ等として使用するメインメモリである。なお、このＳＤＲＡＭ２０３の代わりに、ＤＲＡＭやＳＲＡＭを使用してもよい。

【００５３】

フラッシュメモリ２０４は、例えば図５に示すように、この画像形成装置１００を起動させるブートローダ（ブートプログラム）やＯＳのファイルであるＯＳイメージを記憶するプログラムメモリ、中央管理装置１０２との通信時のＳＳＬによる相互認証に用いるデジタル証明書（以下単に「証明書」ともいう）を記憶する証明書メモリ、各サービス実現のための通信時のＳＳＬによる相互認証に用いる共通のデジタル証明書（以下単に「共通証明書」ともいう）を記憶する共通証明書メモリ、種々の固定パラメータを記憶する固定パラメータメモリ等として使用する不揮発性メモリ（記憶手段）であり、電源がオフになっても記憶内容を保持するようになっている。なお、このフラッシュメモリ２０４の代わりに、ＲＡＭと電池を利用したバックアップ回路を集積した不揮発性ＲＡＭや、ＥＥＰＲＯＭ等の他の不揮発性メモリを使用してもよい。

【００５４】

ＮＲＳ用メモリ２０５は、後述するＮＲＳを記憶する不揮発性メモリであり、オプションでＮＲＳ機能を追加することができる。

ＰＨＹ２０６は、ＬＡＮを介して外部装置と通信を行うためのインタフェースである。

ＮＶＲＡＭ２０７は、例えば図６に示すように、この画像形成装置１００の識別情報である機種機番を記憶する機種機番メモリ、操作部２０９による操作上の初期値を記憶するメモリ、各アプリ（ＡＰＬ）の初期値を記憶するメモリ、各カウンタ情報（課金カウンタのデータ）を記憶するメモリ、上述した共通証明書を記憶する共通証明書メモリ等として使用する不揮発性メモリ（記憶手段）であり、電源がオフになっても記憶内容を保持するようになっている。なお、このＮＶＲＡＭ２０７として、ＲＡＭと電池を利用したバックアップ回路を集積した不揮発性ＲＡＭや、ＥＥＰＲＯＭ，フラッシュメモリ等の不揮発性メモリを使用することができる。

【００５５】

操作部２０９は、操作表示手段（操作手段および表示手段）である。

ＨＤＤ２１０は、電源のオン・オフに関係なくデータを記憶保存する記憶手段（記録媒体）である。このＨＤＤ２１０に、上述したフラッシュメモリ２０４内のプログラムやそれ以外のデータ、あるいはＮＶＲＡＭ２０７内のデータを記憶しておくこともできる。

モデム２１１は、変復調手段であり、中央管理装置１０２へ公衆回線経由でデータを送信する場合、そのデータを公衆回線に流せる形に変調する。また、管理装置１０２から送られてくる変調されたデータを受信した場合、そのデータを復調する。

【００５６】

ＰＩ２１２は、ＲＳ４８５規格に準拠したインタフェースを備え、図示しないラインアダプタを介して公衆回線に接続している。

ＦＣＵ２１３は、ＦＡＸ装置又はモデム機能（ＦＡＸ通信機能）を有するデジタル複写機やデジタル複合機等の画像形成装置および中央管理装置１０２等の外

部装置との通信を公衆回線経由で制御する。

ここで、電源投入（電源オン）により、ＣＰＵ２０１は、ＡＳＩＣ２０２経由でフラッシュメモリ２０４内のブートローダを起動させ、そのブートローダに従い、フラッシュメモリ２０４内のＯＳイメージを読み出し、それをＳＤＲＡＭ２０３にロードして使用可能なＯＳに展開する。そして、ＯＳの展開が完了すると、そのＯＳを起動させる。その後、必要に応じてフラッシュメモリ２０４内のアプリ等のプログラムあるいはＮＲＳ用メモリ２０５内のＮＲＳを読み出し、それをＳＤＲＡＭ２０３にロードして展開し、起動させることにより、各種機能を実現することができる。

【００５７】

次に、画像形成装置１００（又は１１０）におけるソフトウェア構成を図７を用いて説明する。

図７は、画像形成装置１００のソフトウェア構成の一例を示すブロック図である。当該画像形成装置１００のソフトウェア構成は、最上位のアプリケーションモジュール層、その下位のサービスモジュール層からなる。そして、これらのソフトウェアを構成するプログラムはフラッシュメモリ２０４やＮＲＳ用メモリ２０５に記憶され、必要に応じて読み出されてＣＰＵ２０１によって実行される。

【００５８】

アプリケーションモジュール層のソフトウェアは、ＣＰＵ２０１を、ハードウェア資源を動作させて所定の機能を実現させる複数のアプリケーション制御手段（処理実行手段）として機能させるためのプログラムによって構成され、サービスモジュール層のソフトウェアは、ＣＰＵを、ハードウェア資源と各アプリケーション制御手段との間に介在し、複数のアプリケーション制御手段からのハードウェア資源に対する動作要求の受付，その動作要求の調停，およびその動作要求に基づく動作の実行制御を行うサービス制御手段（処理実行手段）として機能させるためのプログラムによって構成される。

【００５９】

なお、それらの機能のうち、中央管理装置１０２との通信に係わる機能（通信手段としての機能）の実現方法は、画像形成装置１００と画像形成装置１１０と

によって異なる。つまり、画像形成装置１１０の場合は、仲介装置１０１の機能を備えているため、ＣＰＵが対応するプログラムを実行することにより、中央管理装置１０２との通信に係わる機能を実現することができる。画像形成装置１００の場合には、ＣＰＵが対応するプログラムを実行すると共に、仲介装置１０１を利用することにより、中央管理装置１０２との通信に係わる機能を実現することができる。

【００６０】

サービスモジュール層には、オペレーションコントロールサービス（ＯＣＳ）３００、エンジンコントロールサービス（ＥＣＳ）３０１、メモリコントロールサービス（ＭＣＳ）３０２、ネットワークコントロールサービス（ＮＣＳ）３０３、ファクスコントロールサービス（ＦＣＳ）３０４、ニューリモートサービス（ＮＲＳ）３０５、システムコントロールサービス（ＳＣＳ）３０６、システムリソースマネージャ（ＳＲＭ）３０７、イメージメモリハンドラ（ＩＭＨ）３０８、カスタマーサポートシステム（ＣＳＳ）３１５、デリバリーコントロールサービス（ＤＣＳ）３１６、ユーザコントロールサービス（ＵＣＳ）３１７を実装している。更に、アプリケーションモジュール層には、コピーアプリ３０９、ファクスアプリ３１０、プリンタアプリ３１１、スキャナアプリ３１２、ネットファイルアプリ３１３、ウェブアプリ３１４を実装している。

【００６１】

これらを更に詳述する。

ＯＣＳ３００は、操作部２０９を制御するモジュールである。

ＥＣＳ３０１は、ハードウェアリソース等のエンジンを制御するモジュールである。

ＭＣＳ３０２は、メモリ制御をするモジュールであり、例えば、画像メモリの取得及び開放、ＨＤＤ２０１の利用等を行う。

ＮＣＳ３０３は、ネットワークとアプリケーションモジュール層の各アプリケーションプログラムとの仲介処理を行わせるモジュールである。

ＦＣＳ３０４は、ファクシミリ送受信、ファクシミリ読み取り、ファクシミリ受信印刷等を行うモジュールである。

【００６２】

ＮＲＳ３０５は、ネットワークを介してデータを送受信する際のデータの変換等をするモジュールであり、またネットワークを介した遠隔管理に関する機能（中央管理装置１０２との通信に係わる機能）をまとめたモジュールである。

ＳＣＳ３０６は、コマンドの内容に応じたアプリケーションモジュール層の各アプリケーションプログラムの起動管理及び終了管理を行うモジュールである。

ＳＲＭ３０７は、システムの制御及びリソースの管理を行うモジュールである。

ＩＭＨ３０８は、一時的に画像データを入れておくメモリを管理するモジュールである。

【００６３】

ＣＳＳ３１５は、公衆回線を介してデータを送受信する際のデータの変換等をするモジュールであり、また公衆回線を介した遠隔管理に関する機能をまとめたモジュールである。

ＤＣＳ３１６は、ＨＤＤ２１０やＳＤＲＡＭ２０３に記憶している（する）画像ファイル等をＳＭＴＰ（Simple Mail Transfer Protocol）やＦＴＰ（File Transfer Protocol）を用いて送受信するモジュールである。

ＵＣＳ３１７は、ユーザが登録した宛先情報や宛名情報等のユーザ情報を管理するモジュールである。

【００６４】

コピーアプリ３０９は、コピーサービスを実現するためのアプリケーションプログラムである。

ファクスアプリ３１０は、ファクスサービスを実現するためのアプリケーションプログラムである。

プリンタアプリ３１１は、プリンタサービスを実現するためのアプリケーションプログラムである。

【００６５】

スキャナアプリ３１２は、スキャナサービスを実現するためのアプリケーションプログラムである。

ネットファイルアプリ３１３は、ネットファイルサービスを実現するためのアプリケーションプログラムである。

ウェブアプリ３１４は、ウェブサービスを実現するためのアプリケーションプログラムである。

【００６６】

次に、上述した画像形成装置１００のソフトウェアの構成に含まれるＮＲＳモジュールの内部構成を図８を用いて更に説明する。

図８は、ＮＲＳモジュールの構成の一例を示す機能ブロック図である。同図に示すように、ＮＲＳ３０５は、ＳＣＳ３０６とＮＣＳ３０３との間で処理をおこなっている。ウェブサーバ機能部５００は、外部から受信した要求に関する応答処理を行う。ここでの要求は、例えば、構造化言語であるＸＭＬ（Extensible Markup Language）形式で記載された、ＳＯＡＰ（Simple Object Access Protocol）によるＳＯＡＰリクエストであることが考えられる。ウェブクライアント機能部５０１は、外部への要求を発行する処理を行う。ｌｉｂｓｏａｐ５０２は、ＳＯＡＰを処理するライブラリであり、ｌｉｂｘｍｌ５０３は、ＸＭＬ形式で記載されたデータを処理するライブラリである。また、ｌｉｂｇｗｗｗ５０４は、ＨＴＴＰを処理するライブラリであり、ｌｉｂｇｗ＿ｎｃｓ５０５は、ＮＣＳ３０３との間の処理をするライブラリである。

【００６７】

図９は、中央管理装置１０２内の物理的構成例を示すブロック図である。

この中央管理装置１０２は、モデム６０１，通信端末６０２，プロキシ（Ｐｒｏｘｙ）サーバ６０３，操作者端末６０４，外部接続Ｉ／Ｆ６０５，ファイルサーバ６０６，デジタル証明書管理装置（以下単に「証明書管理装置」ともいう）６０７，制御装置６０８等からなる。

モデム６０１は、図示しない公衆回線を介して機器利用者側（例えば画像形成装置を利用しているユーザ先）の仲介装置１０１又は画像形成装置１１０と通信するものであり、送受信するデータを変復調する。このモデム６０１と後述する通信端末６０２により通信手段としての機能を果たす。

【００６８】

通信端末６０２は、モデム６０１による通信を制御するものである。

プロキシサーバ６０３は、インタネット１０３を介して機器利用者側の仲介装置１０１又は画像形成装置１１０との通信およびセキュリティ管理を行う。このプロキシサーバ６０３も、通信手段としての機能を果たす。

操作者端末６０４は、各種データの入力をオペレータによるキーボード等の入力装置上の操作により受け付ける。入力されるデータとしては、例えば、各機器利用者側の仲介装置１０１又は画像形成装置１１０と通信する際に使用するそれらのＩＰアドレスや電話番号（発呼先電話番号）等の顧客情報がある。

【００６９】

外部接続Ｉ／Ｆ６０５は、図３の生産工場Ｅ内の通信端末１５０と接続するためのインタフェースである。

ファイルサーバ６０６は、図示しないハードディスク装置等の記憶装置を備え、そこに各機器利用者側の仲介装置１０１および画像形成装置１１０のＩＰアドレスや電話番号、それらの装置から受信したデータ、操作者端末６０４から入力されたデータ、およびこの発明に係わるプログラム等の各種データをそれぞれデータベース（ＤＢ）として記憶している。

【００７０】

証明書管理装置６０７は、生産工場Ｅ内の通信端末１５０からの送信要求により、上述した証明書や共通証明書を発行し、それを中央管理装置１０２へ送信するものである。これについては、追って詳細に説明する。

制御装置６０８は、図示しないＣＰＵ，ＲＯＭ，ＲＡＭ等からなるマイクロコンピュータを備えており、中央管理装置１０２全体を統括的に制御する。そのＣＰＵが、上記プログラムに従って動作する（上記プログラムを必要に応じて実行する）と共に、モデム６０１，通信端末６０２，又はプロキシサーバ６０３を必要に応じて選択的に使用することにより、各種処理を行うことができる。

【００７１】

図１０は、図３の生産工場Ｅの内部構成例を示すブロック図である。

この生産工場Ｅには、生産管理システム１４０，通信端末１５０，工場端末１６０が設置されている。

生産管理システム１４０は、画像形成装置１００，１１０，仲介装置１０１等の通信装置（又はそれらの通信装置に設けられる制御基板）の日々の生産台数を管理する。

通信端末１５０は、生産管理システム１４０からその日の通信装置の機種機番（機種コードとシリアル番号とを含めた情報）別の生産台数を入手（取得）し、その情報に基づいて中央管理装置１０２内の証明書管理装置６０７（認証局に相当する）から必要な証明書を入手する。

【００７２】

工場端末１６０は、バーコードリーダ１４１によって読み取られたバーコードによる機種機番が入力された場合に、その機種機番に対応する証明書を通信端末１５０から入手し、それを対応する通信装置へ送信してその通信装置の不揮発性メモリ（記憶手段）に書き込ませる。

ここで、通信端末１５０および工場端末１６０により、この発明による情報処理装置を構成する。

バーコードリーダ１４１は、読取手段であり、通信装置に貼付された定格銘板あるいは対応するチェックシート上の機種機番（識別情報）を示すバーコードの情報を読み取って工場端末１６０へ送信する。このバーコードリーダ１４１として、ハンドタイプの小型バーコードリーダがある。

【００７３】

図１１は、証明書管理装置６０７のハードウェア構成例を示すブロック図である。

証明書管理装置６０７は、ＣＰＵ１３１，ＲＯＭ１３２，ＲＡＭ１３３（記憶手段），ＨＤＤ１３４（記憶手段），通信Ｉ／Ｆ１３５を備え、これらがシステムバス１３６によって接続されている。

この証明書管理装置６０７によれば、ＣＰＵ１３１がＲＯＭ１３２やＨＤＤ１３４に記憶されている各種制御プログラムを実行することによってこの証明書管理装置６０７の動作を制御し、この発明による機能（デジタル証明書生成手段，デジタル証明書送信手段としての機能）を実現することができる。

【００７４】

図１２は、通信端末１５０のハードウェア構成例を示すブロック図である。

通信端末１５０は、ＣＰＵ１５１，ＲＯＭ１５２，ＲＡＭ１５３，ＨＤＤ１５４，通信Ｉ／Ｆ１５５，入力装置（入力手段）１５６，表示装置（表示手段）１５７を備え、これらがシステムバス１５８によって接続されている。

図１３は、工場端末１６０のハードウェア構成例を示すブロック図である。

工場端末１６０は、ＣＰＵ１６１，ＲＯＭ１６２，ＲＡＭ１６３，通信Ｉ／Ｆ１６４を備え、これらがシステムバス１６６によって接続されている。

【００７５】

通信端末１５０および工場端末１６０によれば、ＣＰＵ１５１がＲＯＭ１５２やＨＤＤ１５４に記憶されている各種制御プログラムを実行することによって通信端末１５０の動作を、ＣＰＵ１６１がＲＯＭ１３２やＨＤＤ１３４に記憶されている各種制御プログラムを実行することによって工場端末１６０の動作をそれぞれ制御し、この発明による機能（デジタル証明書送信要求手段，デジタル証明書送信手段，デジタル証明書保存手段，書き込み済み情報設定手段，デジタル証明書削除手段としての機能等）を実現することができる。

なお、証明書管理装置６０７，通信端末１５０，工場端末１６０のハードウェアとしては、適宜公知のコンピュータを採用することができる。もちろん、必要に応じて他のハードウェアを付加してもよい。

【００７６】

図１４は、生産工場Ｅにおける通信端末１５０および工場端末１６０の周辺を示すブロック図である。

通信端末１５０は、セキュリティ面を考慮し、生産工場Ｅの管理者室Ｆに設置されている。その管理者室Ｆは、特定の管理者しか入れないように、ドアＧに鍵をかけるようにしている。また、通信端末１５０は、特定のＩＤ，パスワードが入力された場合にのみ、操作できるようにしている。

この例では、生産工場Ｅには、仲介装置１０１の生産用ライン１００１，画像形成装置１００の生産用ライン１００２，画像形成装置１１０の生産用ライン１００３がある。そして、その各生産用ライン１００１，１００２，１００３毎に工場端末１６０（１６０ａ，１６０ｂ，１６０ｃ）が設置されている。

【００７７】

各工場端末１６０にはそれぞれ、バーコードリーダ１４１（１４１ａ，１４１ｂ，１４１ｃ）と接続するためのバーコード用Ｉ／Ｆ１４２（１４２ａ，１４２ｂ，１４２ｃ）、および通信装置（仲介装置１０１，画像形成装置１００，１１０）と接続するための書き込み用Ｉ／Ｆ１６５（１６５ａ，１６５ｂ，１６５ｃ）がそれぞれ接続されている。

図１５は、工場端末１６０とバーコードリーダ１４１と通信装置との接続例を示す図である。

【００７８】

この図１５を見て分かるように、工場端末１６０ｂに、バーコード用Ｉ／Ｆ１４２ｂを介してバーコードリーダ１４１ｂが、書き込み用Ｉ／Ｆ１６５を介して画像形成装置１００がそれぞれ接続されている。

なお、画像形成装置１００（又は画像形成装置１１０や仲介装置１０１）は、初期値として同じＩＰアドレスを有しており、工場端末１６０とＬＡＮ接続すると、ＩＰアドレスが重複してしまうため、クロスケーブル（書き込み用Ｉ／Ｆ１６５を使用して工場端末１６０と接続している。

図１６は、画像形成装置１００又は１１０に貼付された定格銘板の一例を示す図である。

この定格銘板の機種機番を示すバーコードＢＣの情報を、バーコードリーダ１４１によって読み取ることができる。

【００７９】

図１７は、図１４に示した生産工場Ｅの各生産用ライン１００１，１００２，１００３での通信装置の生産工程の一例を示す説明図である。

各生産用ライン１００１，１００２，１００３ではそれぞれ、まず通信装置（仲介装置１０１，画像形成装置１００，１１０）の制御基板が組み立てられ、次にその制御基板の検査が行われた後、工場端末１６０によって固定値を共通証明書としてフラッシュメモリ２０４およびＮＶＲＡＭ２０７に書き込まれる。

その後、フラッシュメモリ２０４およびＮＶＲＡＭ２０７に共通証明書が書き込まれた制御基板が梱包され、サービス部品として出荷される。

【００８０】

あるいは、フラッシュメモリ２０４およびＮＶＲＡＭ２０７に共通証明書が書き込まれた制御基板は、製品用として次工程へ送られる。そして、その制御基板は予め組み立てられた画像形成装置１００又は１１０のカバーに合わせられ、その画像形成装置１００又は１１０に搭載され、製品が出来あがる。

その製品となった画像形成装置１００又は１１０は、その機能検査が行われた後、通信端末１５０および工場端末１６０によって証明書がフラッシュメモリ２０４に書き込まれると共に、フラッシュメモリ２０４内のパラメータが初期化される。

その後、その画像形成装置１００又は１１０は、外観が検査された後、梱包され、出荷される。

なお、制御基板の組み立てと製品の組み立ては、別工場で行うことが多い。

【００８１】

次に、上述した画像形成装置管理システム（情報管理システム）における実施形態、つまりこの発明の特徴となる動作（証明書取得処理）について、図１８～図２３を参照して具体的に説明する。

図１８は、この画像形成装置遠隔管理システムにおける証明書取得処理時の通信シーケンスの一例を示す図である。

図１９は、通信端末１５０のＨＤＤ１５４内の工場製造管理ＤＢの一例を示す図である。

図１９の（ａ）は証明書管理機器一覧ＤＢの一例を示しており、機種コード別の証明書の有無を示している。同図の（ｂ）は生産計画ＤＢの一例を示しており、機種コード別の日々の生産台数を示している。

【００８２】

図２０は、通信端末装置１５０のＨＤＤ１５４内の証明書ＤＢ１５４ａの一例を示す図である。

証明書ＤＢ１５４ａは、機種機番別の証明書，その作成日，その書き込み済みフラグの状態を示している。そのうち、証明書（デジタル証明書）は、ルート証明書（ルート鍵証明書），クライアント証明書（クライアント公開鍵証明書），

秘密鍵（クライアント私有鍵）のパックになっている。

図２１は、証明書管理装置６０７と通信端末１５０との通信時のデータフォーマットの一例を示す図である。

図２２は、通信端末１５０と工場端末１６０との通信時のデータフォーマットの一例を示す図である。

図２３は、工場端末１６０と通信装置（画像形成装置１００等）との通信時のデータフォーマットの一例を示す図である。

【００８３】

通信端末１５０のＣＰＵ１５１は、毎月、所定のタイミングで（予め決められた日時に）生産管理システム１４０から各通信装置（画像形成装置１００等）の日々の生産台数を取得し、ＨＤＤ１５４内の生産計画ＤＢに保存することにより、その生産計画ＤＢを更新する。

を更新する。また、毎日、所定のタイミングで（予め決められた時刻）に、ＨＤＤ１５４内の証明書管理機器一覧ＤＢおよび生産計画ＤＢに基づいて、本日生産（製造）された各通信装置による通信時のＳＳＬによる相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）を本日の生産台数分だけ付加して証明書管理装置６０７へ通知する。なお、１台の通信装置毎に通信要求を通知することもできる。

【００８４】

証明書管理装置６０７のＣＰＵ１３１は、通信端末１５０から証明書の送信要求を受けた場合に、その送信要求に付加された機種機番を含む証明書をその機種機番数だけ生成し、その各証明書を通信端末１５０へ送信する。

なお、通信端末１５０と証明書管理装置６０７とは、共通証明書を用いてＳＳＬによる相互認証を行った後、図２１に示すようなＳＯＡＰ（構造化言語形式であるＸＭＬ形式）によるデータフォーマットでＳＳＬ通信を行うようにしている。

通信端末１５０のＣＰＵ１５１は、証明書管理装置６０７への各機種機番を含む証明書の送信要求に対して、その証明書管理装置６０７からその各機種機番をそれぞれ含む各証明書を受信すると、それらの証明書をＨＤＤ１５４内の証明書

ＤＢ１５４ａに保存することにより、その証明書ＤＢを更新する。

【００８５】

工場端末１６０のＣＰＵ１６１は、本日生産された各通信装置に貼付された定格銘板あるいは対応するチェックシートから機種機番を示すバーコードがバーコードリーダ１４１によって順次読み取られ、その各バーコードによる機種機番が順次入力されると、その入力順に、そのバーコードによる機種機番を含む証明書の送信要求を通信端末１５０へ通知する。

通信端末１５０のＣＰＵ１５１は、工場端末１６０からバーコードによる機種機番を含む証明書の送信要求を受けた場合に、その機種機番に対応する証明書をＨＤＤ１５４内の証明書ＤＢから読み出して工場端末１６０へ送信する。

工場端末１６０のＣＰＵ１６１は、通信端末１５０への機種機番を含む証明書の送信要求に対して、その通信端末１５０から証明書を受信すると、その証明書を該当する通信装置（機種機番が読み取られた通信装置）へ送信する。

【００８６】

通信装置のＣＰＵは、工場端末１６０から証明書を受信すると、受信応答を工場端末１６０へ通知した後、その証明書を内部の不揮発性メモリ（画像形成装置１００の場合はフラッシュメモリ２０４）に書き込み、その書き込みが正常に終了したことを確認できた場合には、証明書の書き込みが完了（成功）した旨を示す書き込み結果を工場端末１６０へ通知する。証明書の書き込みが正常に終了しなかったことを確認できた場合には、証明書の書き込みが失敗した旨を示す書き込み結果を工場端末１６０へ通知する。

工場端末１６０のＣＰＵ１６１は、該当する通信装置への証明書の送信に対して、その通信装置から受信応答の通知を受けると、その受信応答を通信端末１５０へ通知する。続いて、書き込み結果の通知を受けると、その書き込み結果を通信端末１５０へ通知する。

【００８７】

通信端末１５０のＣＰＵ１５１は、工場端末１６０への証明書の送信に対して、工場端末１６０から受信応答の通知に続いて書き込み結果の通知を受けると、受信応答を工場端末１６０へ通知した後、その書き込み結果から証明書の書き込

みが完了したことを確認できた場合には、証明書ＤＢ１５４ａ（図２０）における対応する証明書（書き込みが完了した証明書）の書き込み済みを示す書き込み済みフラグ（情報）を“１”（済み）にセット（設定）する。証明書の書き込みが失敗したことを確認できた場合には、対応する機種機番を含む証明書の送信要求を証明書管理装置６０７へ通知することにより、上述と同様にして新たな証明書を取得した後、その証明書を通信端末１５０へ通知し、以後上述と同様の処理を行う。

【００８８】

なお、証明書ＤＢ１５４ａに、同じ証明書を長く保持すると、セキュリティの問題もあるため、工場端末１６０から書き込み結果の通知を受けた場合に、対応する証明書を証明書ＤＢ１５４ａから削除するようにしてもよい。

工場端末１６０のＣＰＵ１６１は、通信端末１５０への受信応答および書き込み結果の通知に対して、その通信端末１５０から受信応答の通知を受けると、その受信応答を該当する通信装置へ通知する。

【００８９】

なお、通信端末１５０と工場端末１６０とは、図２２に示すようなＳＯＡＰによるデータフォーマットで通信を行うようにしている。

また、工場端末１６０と該当する通信装置とは、共通証明書を用いてＳＳＬによる相互認証を行った後、図２３に示すようなＳＯＡＰによるデータフォーマットでＳＳＬ通信を行うようにしている。この場合、工場端末１６０のＣＰＵ１６１は該当する通信装置へ送信すべき証明書を暗号化し、その通信装置のＣＰＵは工場端末１６０から受信した暗号化された証明書をそのまま不揮発性メモリに書き込むか、復号化した後不揮発性メモリに書き込むようにしている。

【００９０】

さらに、この実施形態では、各通信装置の機種機番をバーコードリーダによって読み取って工場端末１６０へ入力するようにしているが、例えば信端末１５０の入力装置１５６を操作することにより、各通信装置の機種機番を入力するようにしてもよい。

さらにまた、ある機種の生産が打ち切られた場合には、計画的に処理を行うが

、何らかの事情で通信端末１５０の証明書ＤＢ１５４ａに対応する証明書（生産が打ち切りとなった通信装置の機種に対応する証明書）が残ったままになっていた場合には、管理責任者が通信端末１５０の入力装置１５６を操作することにより、対応する証明書を証明書ＤＢ１５４ａから削除（消去）することもできる。

また、通信端末１５０のＣＰＵ１５１は、現在有している機種毎の証明書の数と当日使用した証明書の数を表示装置１５７に表示させることもできる。

【００９１】

この実施形態においては、以下の（１）～（５）に示す作用効果を得ることができる。

（１）通信端末１５０のＣＰＵ１５１が、生産されたある通信装置によるＳＳＬ通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）をその通信装置の生産台数分だけ付加して証明書管理装置６０７へ通知し、その各機種機番を付加した証明書の要求通知に対して、その証明書管理装置６０７からその各機種機番をそれぞれ含む各証明書を受信した場合に、その各証明書を証明書ＤＢ１５４ａに保存した後、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の機種機番を示すバーコードがバーコードリーダ１４１によって読み取られ、そのバーコードによる機種機番が工場端末１６０経由で入力された場合に、その機種機番に対応する証明書を証明書ＤＢ１５４ａから読み出して工場端末１６０によって上記ある通信装置（機種機番が読み取られた通信装置）へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

それによって、中央管理装置１０２側が、その通信装置とＳＳＬ通信する際の相互認証時に、その通信装置から受信した証明書内の機種機番をチェックすることにより、その通信装置が保守契約したものであるかどうかを正確に判定することが可能になる。

【００９２】

（２）通信端末１５０のＣＰＵ１５１が、生産されたある通信装置によるＳＳＬ通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）をその通信装置の生産台数分だけ付加して証明書管理装置６０７へ通知し、

その各機種機番を付加した証明書の要求通知に対して、その証明書管理装置６０７からその各機種機番をそれぞれ含む各証明書を受信した場合に、その各証明書を証明書ＤＢ１５４ａに保存した後、上記生産台数分の通信装置のいずれかかが入力装置１５６によって入力された場合に、その機種機番に対応する証明書を証明書ＤＢ１５４ａから読み出して工場端末１６０によって上記ある通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

それによって、（１）と同様の効果を得ることができる。但し、入力装置１５６の操作によって機種機番を入力するため、入力ミスしないように注意する必要がある。

【００９３】

（３）（１）又は（２）の工場端末１６０から対応する通信装置への証明書の送信の際に、工場端末１６０のＣＰＵ１６１が、その通信装置との間で共通証明書を用いて相互認証を行い、その通信装置へ送信すべき証明書を暗号化する。

それによって、工場端末１６０と通信装置との間の通信のセキュリティが向上する。

（４）通信端末１５０のＣＰＵ１５１が、対応する通信装置の不揮発性メモリへの証明書の書き込みが完了した場合に、証明書ＤＢ１５４ａにおけるその証明書の書き込み済みを示す書き込み済みフラグを“１”にセットする。

それによって、証明書の書き込みが完了した通信装置を特定することができるため、通信装置の生産性の向上につながる。

【００９４】

（５）通信端末１５０のＣＰＵ１５１が、対応する通信装置の不揮発性メモリへの証明書の書き込みが完了した場合に、その証明書を証明書ＤＢ１５４ａから削除する。

それによって、（４）と同様の効果を得られる。また、証明書ＤＢ１５４ａに、同じ証明書を長く保持すると、セキュリティの問題もあるため、書き込みが完了した証明書を証明書ＤＢ１５４ａから削除すれば、セキュリティの向上につながる。

【００９５】

なお、通信端末１５０のＣＰＵ１５１が、生産されたある通信装置によるＳＳＬ通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）を付加して証明書管理装置６０７へ通知し、その機種機番を付加した証明書の要求通知に対して、その証明書管理装置６０７からその機種機番を含む証明書を受信した場合に、その証明書を工場端末１６０によって上記ある通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませることもできる。このようにすれば、証明書ＤＢ１５４ａをなくすこともでき、低コストにつながる。

【００９６】

以上、この発明を画像形成装置１００，１１０，および仲介装置１０１の不揮発性メモリに証明書を書き込むための通信端末１５０および工場端末１６０に適用した実施形態について説明したが、この発明はこれに限らず、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム等や、ネットワークに接続可能なコンピュータ等の通信装置の不揮発性メモリに証明書を書き込むための情報処理装置に適用可能である。

また、この発明によるプログラムは、通信端末１５０および工場端末１６０を制御するコンピュータ（ＣＰＵ１３１，１５１）に、この発明による各機能（デジタル証明書生成手段，デジタル証明書送信手段，書き込み済み情報設定手段，デジタル証明書削除手段としての機能等）を実現させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

【００９７】

このようなプログラムは、はじめからコンピュータに備えるＲＯＭあるいはＨＤＤ等の記憶手段に格納しておいてもよいが、記録媒体であるＣＤ－ＲＯＭあるいはフレキシブルディスク，ＳＲＡＭ，ＥＥＰＲＯＭ，メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてＣＰＵに実行させるか、ＣＰＵにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外

部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【００９８】

【発明の効果】

以上説明してきたように、この発明によれば、中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定することができる。

【図面の簡単な説明】

【図１】

この発明による通信装置を被管理装置とする遠隔管理システムの構成例を示す概念図である。

【図２】

その遠隔管理システムにおけるデータ送受モデルを示す概念図である。

【図３】

この発明による電子装置を画像形成装置とする画像形成装置遠隔管理システムの構成例を示す概念図である。

【図４】

図３の画像形成装置１００のハードウェア構成例を示すブロック図である。

【図５】

図４のフラッシュメモリ２０４の記憶エリアの構成例を示すメモリマップ図である。

【図６】

図４のＮＶＲＡＭ２０７の記憶エリアの構成例を示すメモリマップ図である。

【図７】

図３の画像形成装置１００（又は１１０）のソフトウェア構成例を示すブロック図である。

【図８】

図７のＮＲＳ３０５の構成例を示す機能ブロック図である。

【図９】

図３の中央管理装置１０２の概略構成例を示すブロック図である。

【図１０】

図３の生産工場Ｅの内部構成例を示すブロック図である。

【図１１】

図１０の証明書管理装置６０７のハードウェア構成例を示すブロック図である。

【図１２】

図１０の通信端末１５０のハードウェア構成例を示すブロック図である。

【図１３】

図１０の工場端末１６０のハードウェア構成例を示すブロック図である。

【図１４】

図１０の生産工場Ｅにおける通信端末１５０および工場端末１６０の周辺を示すブロック図である。

【図１５】

図１０の工場端末１６０とバーコードリーダ１４１と通信装置との接続例を示す図である。

【図１６】

図１０の画像形成装置１００又は１１０に貼付された定格銘板の一例を示す図である。

【図１７】

図１４に示した生産工場Ｅの各生産用ライン１００１，１００２，１００３での通信装置の生産工程の一例を示す説明図である。

【図１８】

図１０の生産工場Ｅ内の通信端末１５０および工場端末１６０による証明書取得処理時の通信シーケンスの一例を示す図である。

【図１９】

図１２のＨＤＤ１５４内の工場製造管理ＤＢの一例を示す図である。

【図２０】

図１２のＨＤＤ１５４内の証明書ＤＢの一例を示す図である。

【図２１】

図１０の証明書管理装置６０７と通信端末１５０との通信時のデータフォーマットの一例を示す図である。

【図２２】

図１０の通信端末１５０と工場端末１６０との通信時のデータフォーマットの一例を示す図である。

【図２３】

図１０の工場端末１６０と通信装置（画像形成装置１００等）との通信時のデータフォーマットの一例を示す図である。

【図２４】

クライアント装置とサーバ装置とがＳＳＬによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図２５】

図２４に示した認証処理におけるルート鍵、ルート私有鍵、およびクライアント公開鍵の関係について説明するための図である。

【符号の説明】

１０：被管理装置　　１１：仲介機能付被管理装置

１００：画像形成装置　　１０１：仲介装置

１０２：管理装置　　１０３：インタネット

１０４：ファイアウォール

１１０：仲介機能付画像形成装置

１３１，１５１，１６１，２０１：ＣＰＵ

１３２，１５２，１６２：ＲＯＭ

１３３，１５３，１６３：ＲＡＭ

１３４，１５４，２１０：ＨＤＤ

１３５，１５５，１６４：通信Ｉ／Ｆ

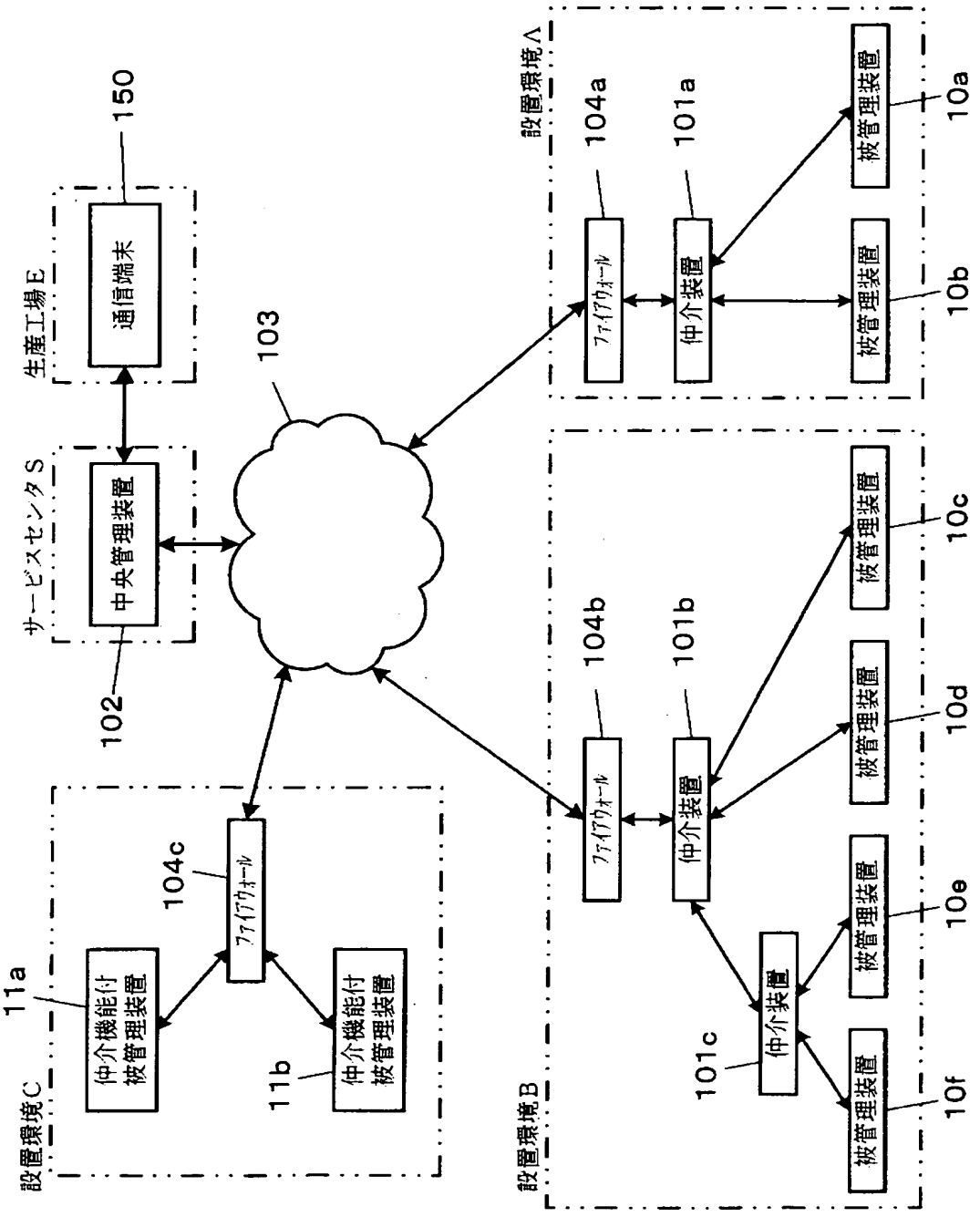
１５６：入力装置　　１５７：表示装置

１４０：生産管理システム　１４１：バーコードリーダ

１５０，６０２：通信端末　１６０：工場端末
２０２：ＡＳＩＣ　２０３：ＳＤＲＡＭ
２０４：フラッシュメモリ　２０５：ＮＲＳ用メモリ
２０６：ＰＨＹ　２０７：ＮＶＲＡＭ
２０９：操作部　２１２：ＰＩ
３００：ＯＣＳ　３０１：ＥＣＳ
３０２：ＭＣＳ　３０３：ＮＣＳ
３０４：ＦＣＳ　３０５：ＮＲＳ
３０６：ＳＣＳ　３０７：ＳＲＭ
３０８：ＩＭＨ　３０９：コピーアプリ
３１０：ファクスアプリ　３１１：プリンタアプリ
３１２：スキャナアプリ
３１３：ネットファイルアプリ　３１４：ウェブアプリ
６０１：モデム
６０３：プロキシサーバ　６０４：操作者端末
６０５：外部接続Ｉ／Ｆ　６０６：ファイルサーバ
６０７：証明書管理装置　６０８：制御装置

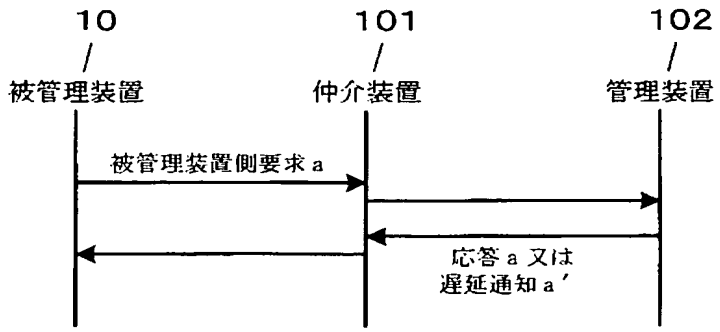
【書類名】　図面

【図１】

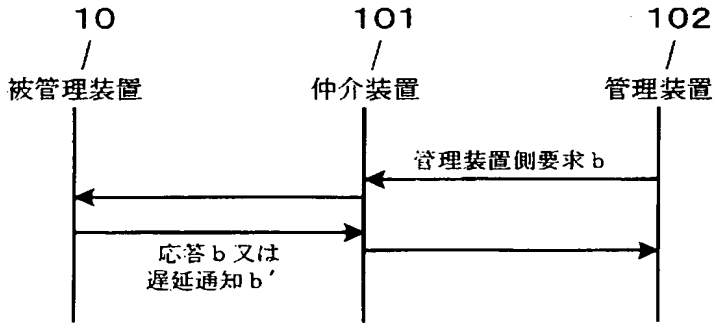

設置環境A
104a
101a
10a
10b
ファイアウォール
仲介装置
被管理装置
生産工場E
150
通信端末
103
サービスセンタS
中央管理装置
102
設置環境B
104b
101b
10c
10d
10e
10f
101c
仲介装置
設置環境C
11a
11b
104c
仲介機能付
被管理装置

【図２】

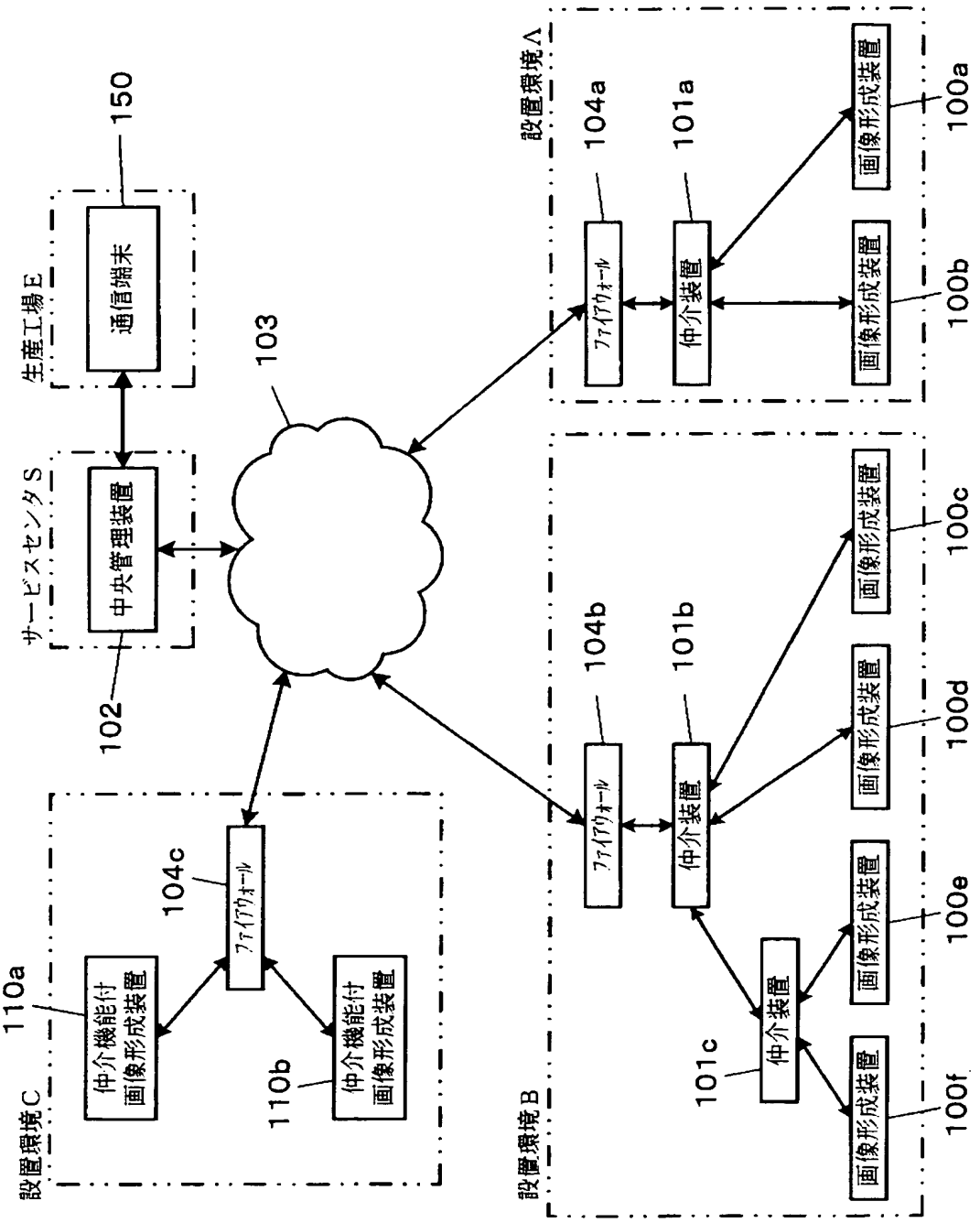
(A)


10
101
102
被管理装置
仲介装置
管理装置
被管理装置側要求ａ
応答ａ又は
遅延通知ａ′

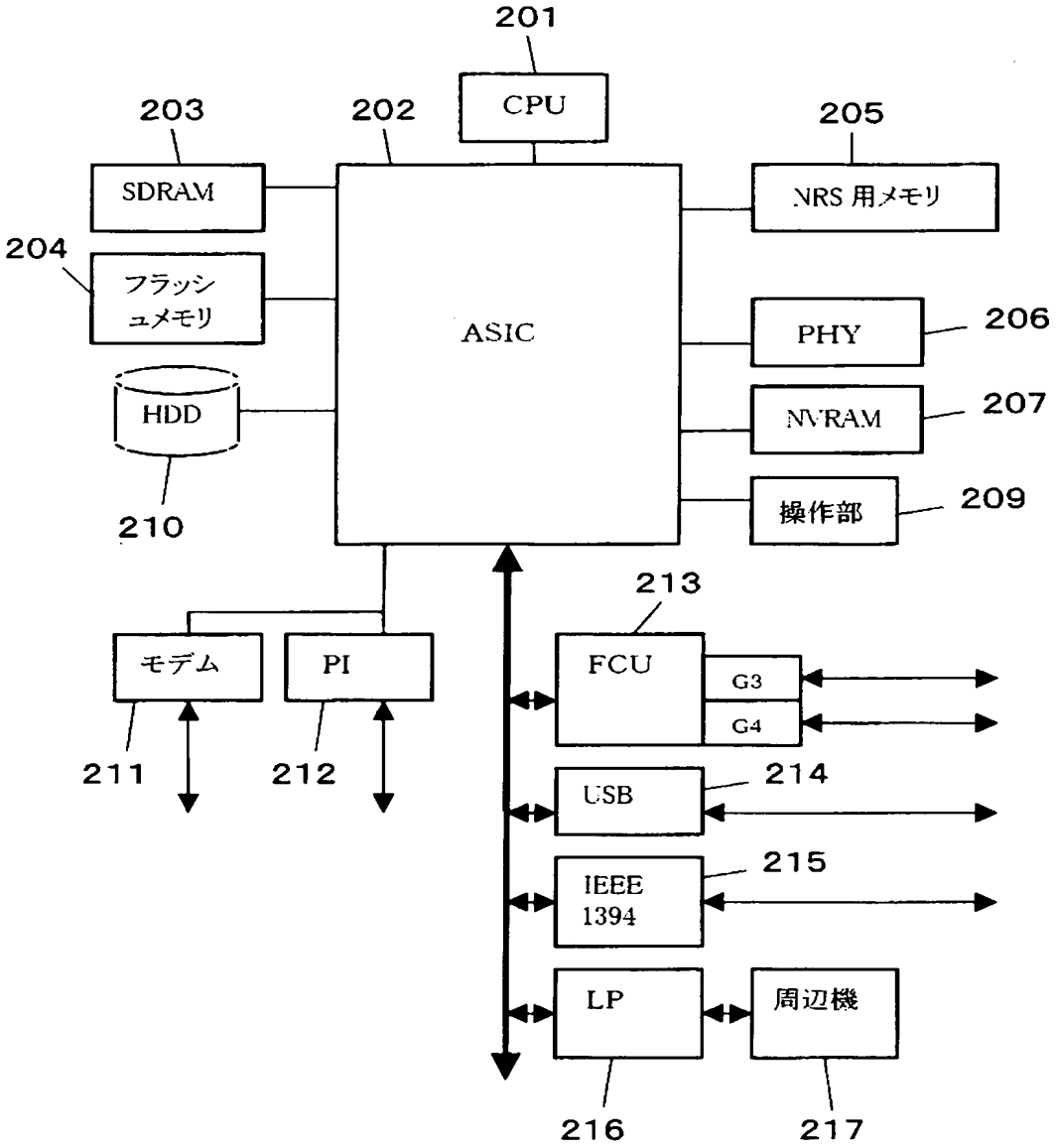
(B)


10
101
102
被管理装置
仲介装置
管理装置
管理装置側要求ｂ
応答ｂ又は
遅延通知ｂ′

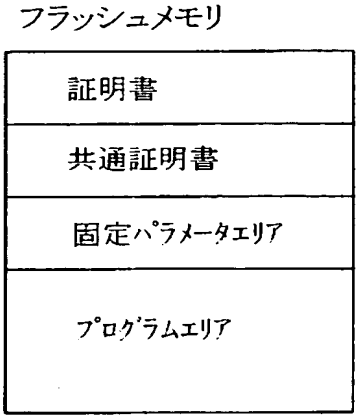
【図３】


設置環境C
サービスセンタS
生産工場E
設置環境A
設置環境B
150
通信端末
103
102
中央管理装置
104a
104b
104c
ファイアウォール
101a
101b
101c
伸介装置
110a
110b
伸介機能付
画像形成装置
100a
100b
100c
100d
100e
100f
画像形成装置

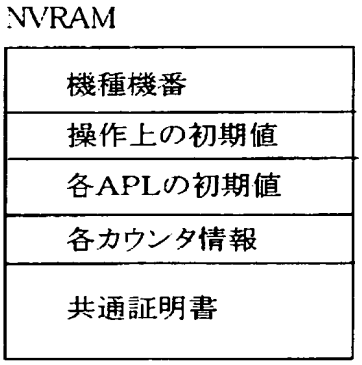
【図４】


201
CPU
203
202
205
SDRAM
NRS 用メモリ
204
フラッシュメモリ
ASIC
PHY
206
HDD
NVRAM
207
210
操作部
209
213
モデム
PI
FCU
G3
G4
211
212
USB
214
IEEE 1394
215
LP
周辺機
216
217

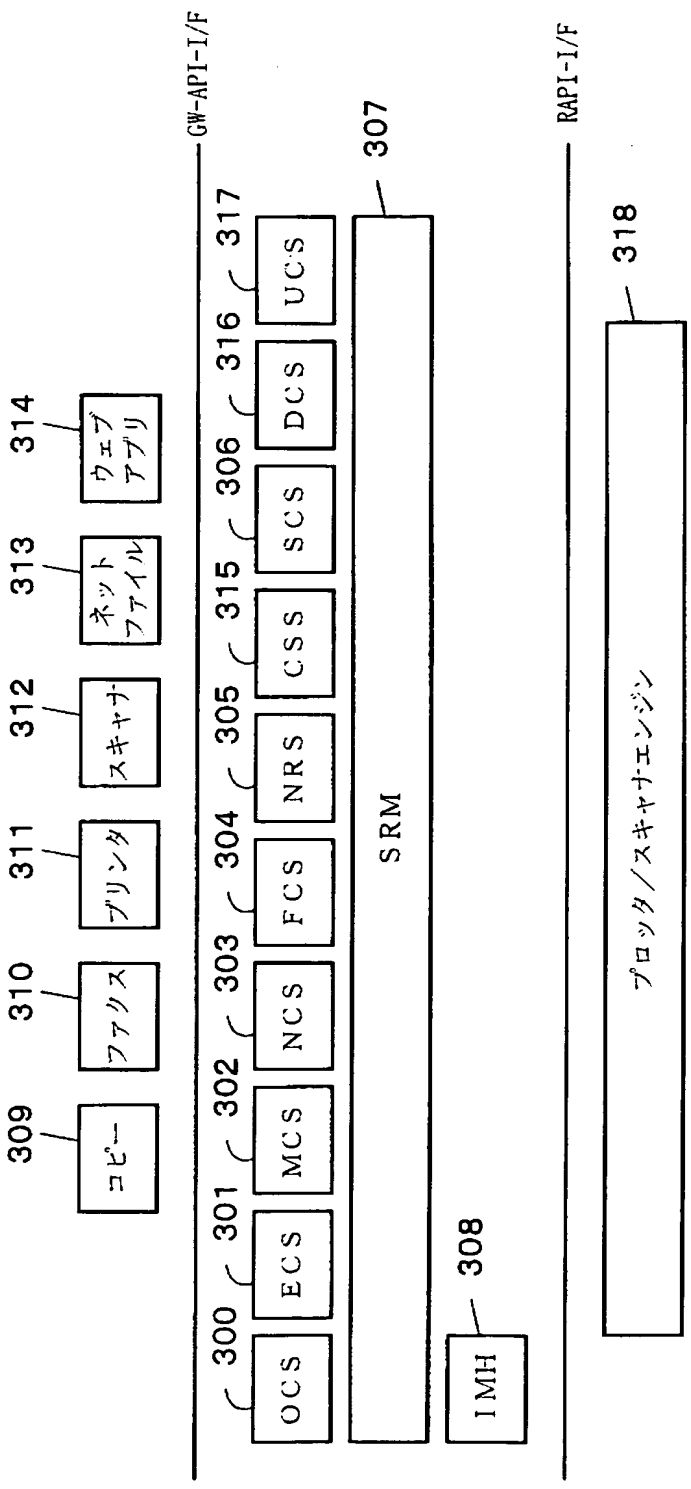
【図５】


フラッシュメモリ
証明書
共通証明書
固定ﾊﾟﾗﾒｰﾀｴﾘｱ
ﾌﾟﾛｸﾞﾗﾑｴﾘｱ

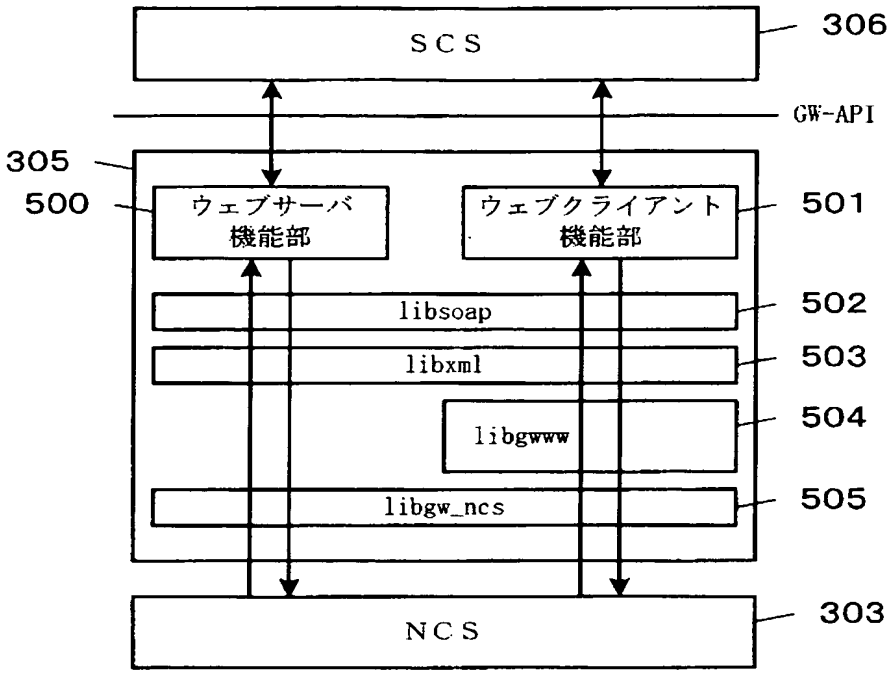
【図６】


NVRAM
機種機番
操作上の初期値
各APLの初期値
各カウンタ情報
共通証明書

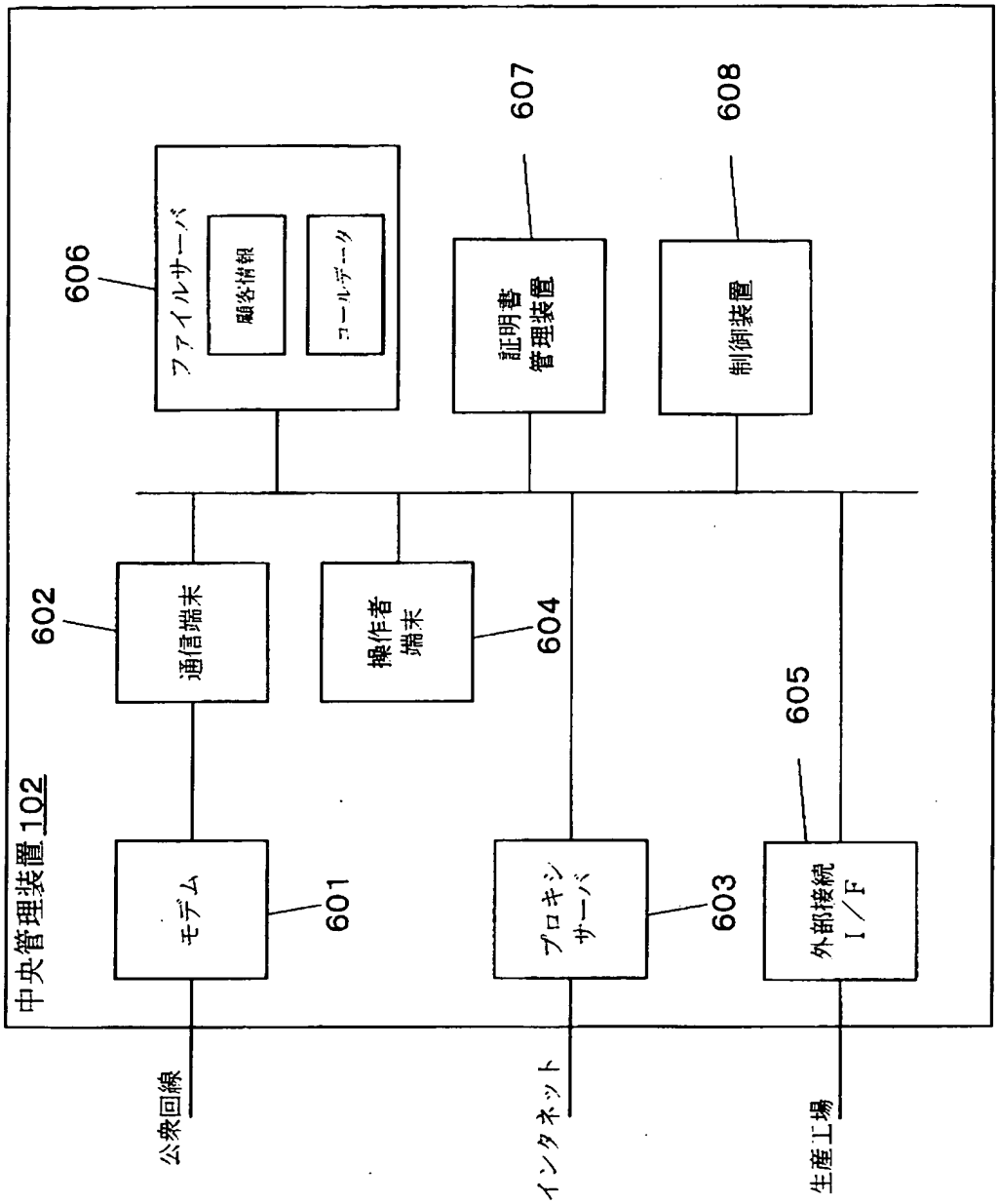
【図７】


GW-API-I/F
RAPI-I/F
309
コピー
310
ファクス
311
プリンタ
312
スキャナ
313
ネットファイル
314
ウェブアプリ
300
OCS
301
ECS
302
MCS
303
NCS
304
FCS
305
NRS
306
SCS
307
SRM
308
IMH
315
CSS
316
DCS
317
UCS
318
プロッタ／スキャナエンジン

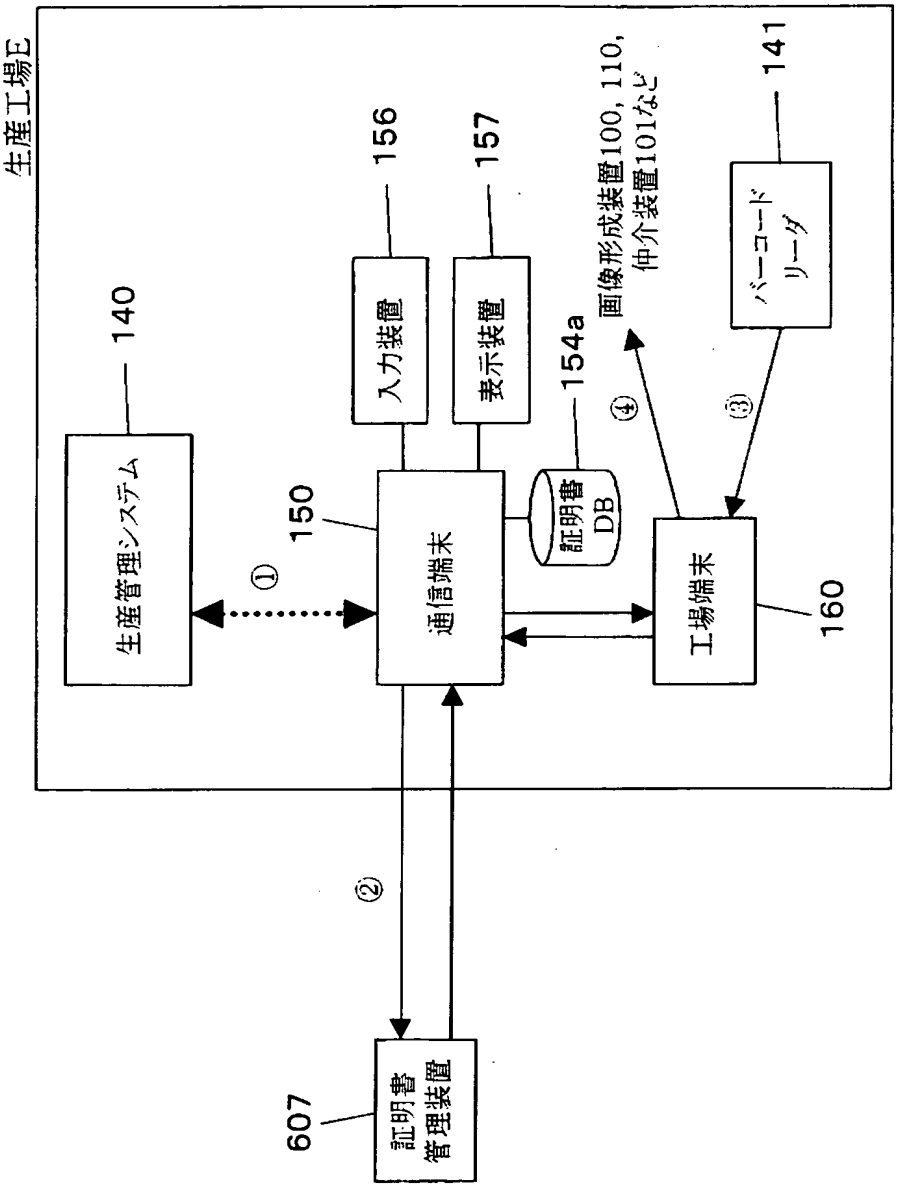
【図８】


SCS
306
GW-API
305
500
ウェブサーバ
機能部
ウェブクライアント
機能部
501
libsoap
502
libxml
503
libgwww
504
libgw_ncs
505
NCS
303

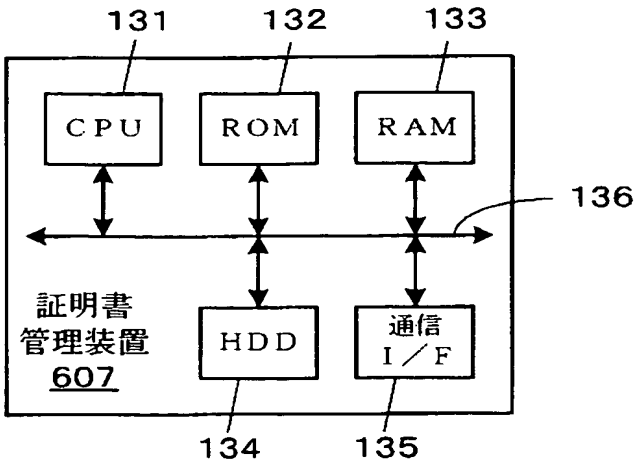
【図９】


中央管理装置102
モデム
601
通信端末
602
操作者端末
604
プロキシサーバ
603
外部接続I／F
605
ファイルサーバ
606
顧客情報
コールデータ
証明書管理装置
607
制御装置
608
公衆回線
インターネット
生産工場

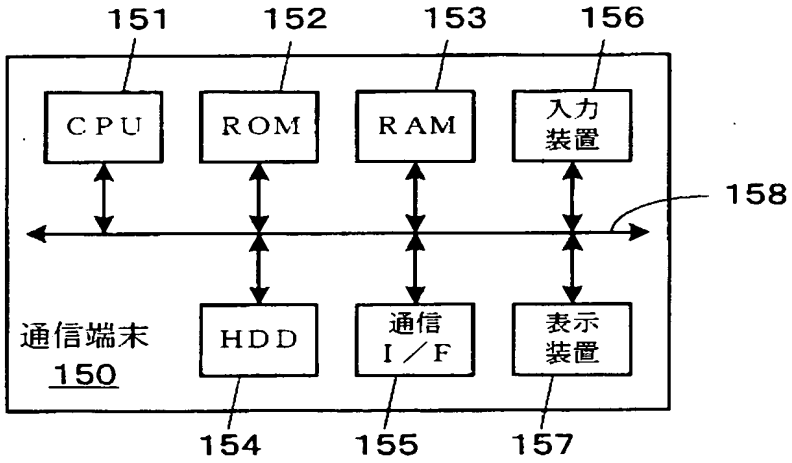
【図１０】


生産工場E
140
生産管理システム
①
150
通信端末
入力装置
156
表示装置
157
154a
証明書DB
画像形成装置100, 110,
仲介装置101など
④
③
バーコードリーダ
141
工場端末
160
②
607
証明書管理装置

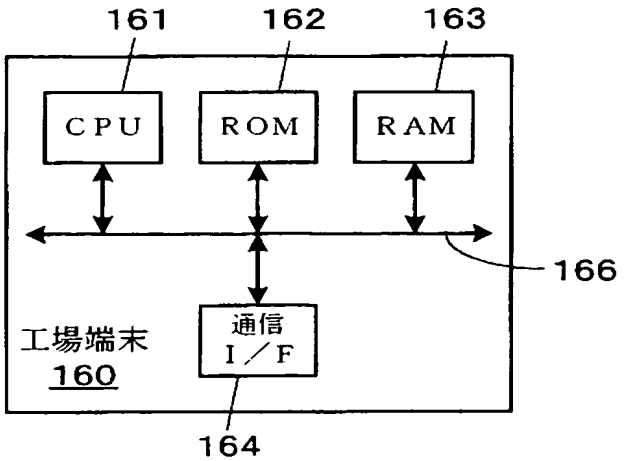
【図１１】


131
132
133
CPU
ROM
RAM
136
証明書
管理装置
607
HDD
通信
I／F
134
135

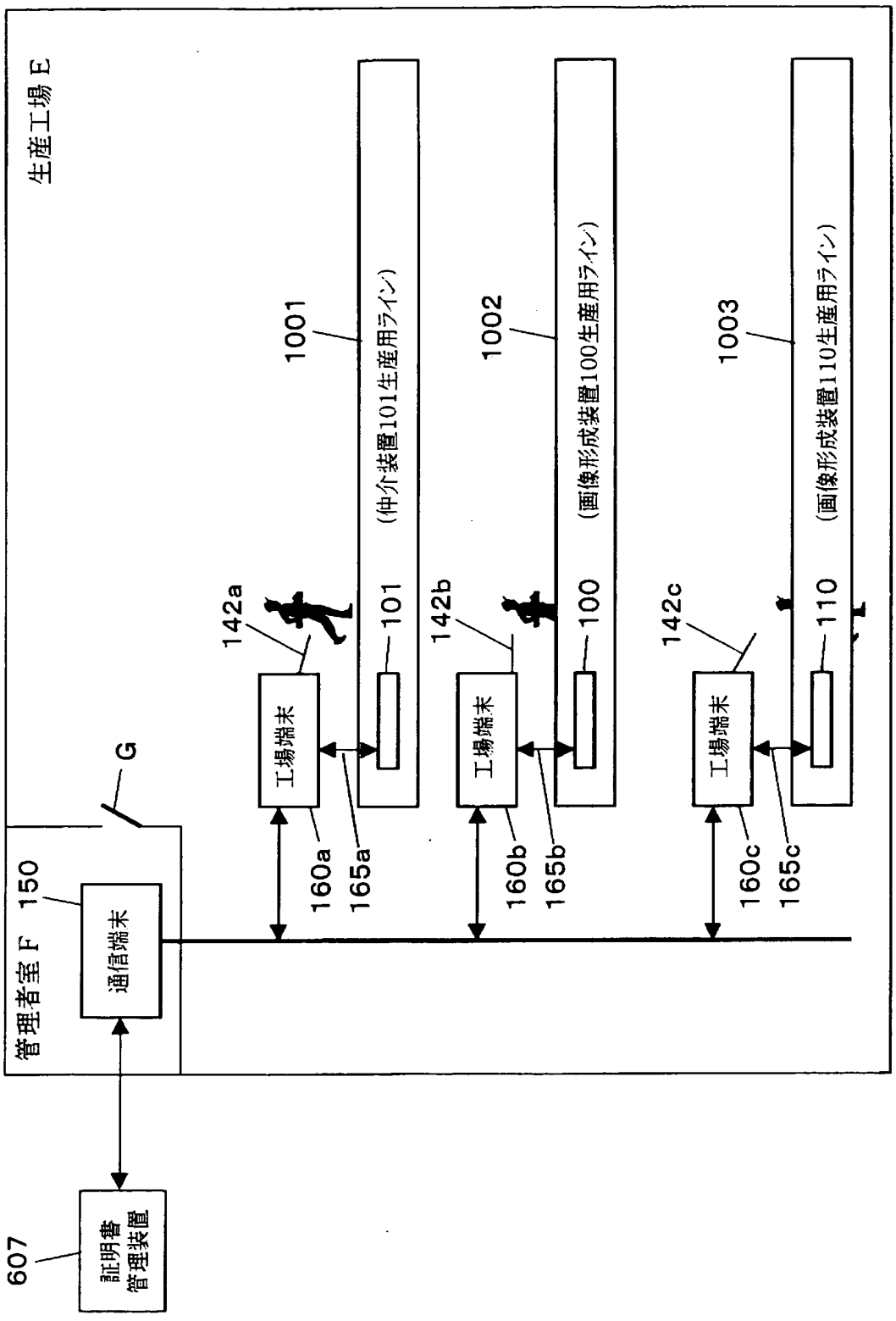
【図１２】


151
152
153
156
CPU
ROM
RAM
入力
装置
158
通信端末
150
HDD
通信
I／F
表示
装置
154
155
157

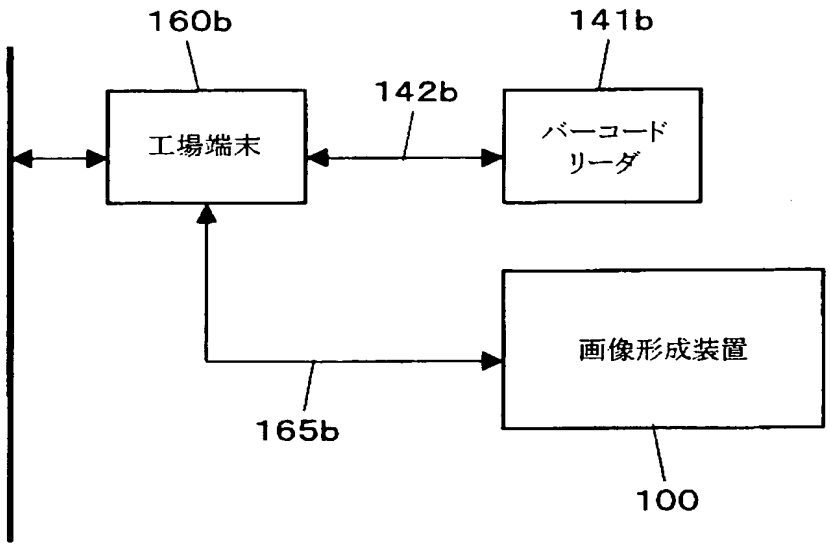
【図１３】


161
162
163
CPU
ROM
RAM
166
工場端末
160
通信
I／F
164

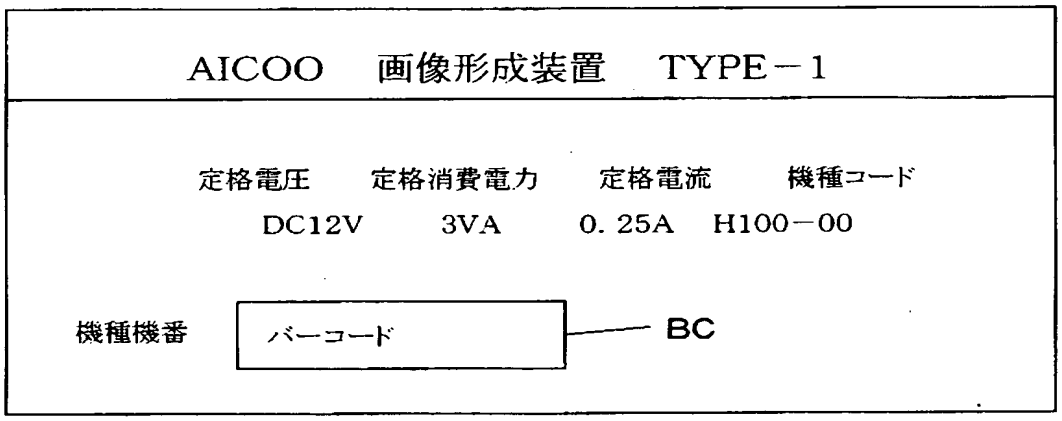
【図１４】


生産工場 E
管理者室 F
150
通信端末
G
607
証明書
管理装置
1001
(仲介装置101生産用ライン)
1002
(画像形成装置100生産用ライン)
1003
(画像形成装置110生産用ライン)
142a
142b
142c
工場端末
工場端末
工場端末
101
100
110
160a
165a
160b
165b
160c
165c

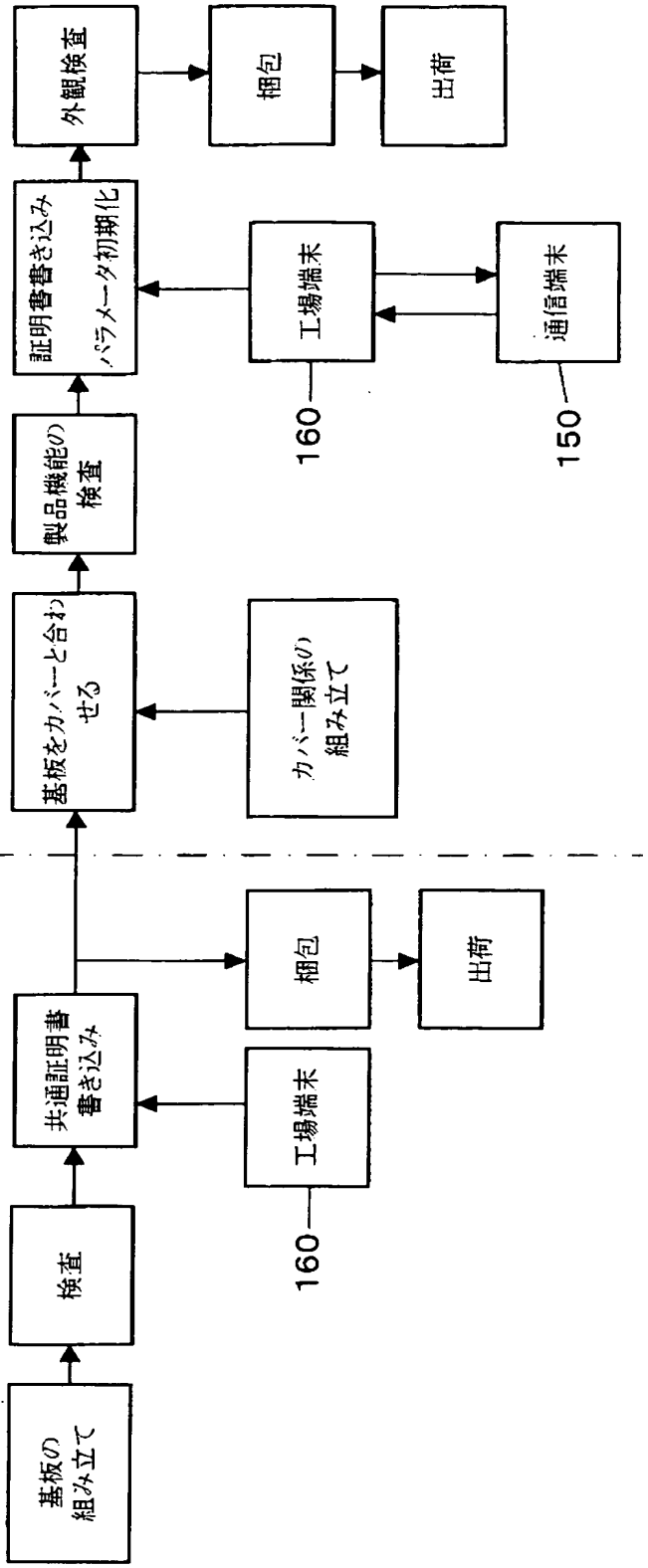
【図１５】


160b
141b
142b
工場端末
バーコード
リーダ
画像形成装置
165b
100

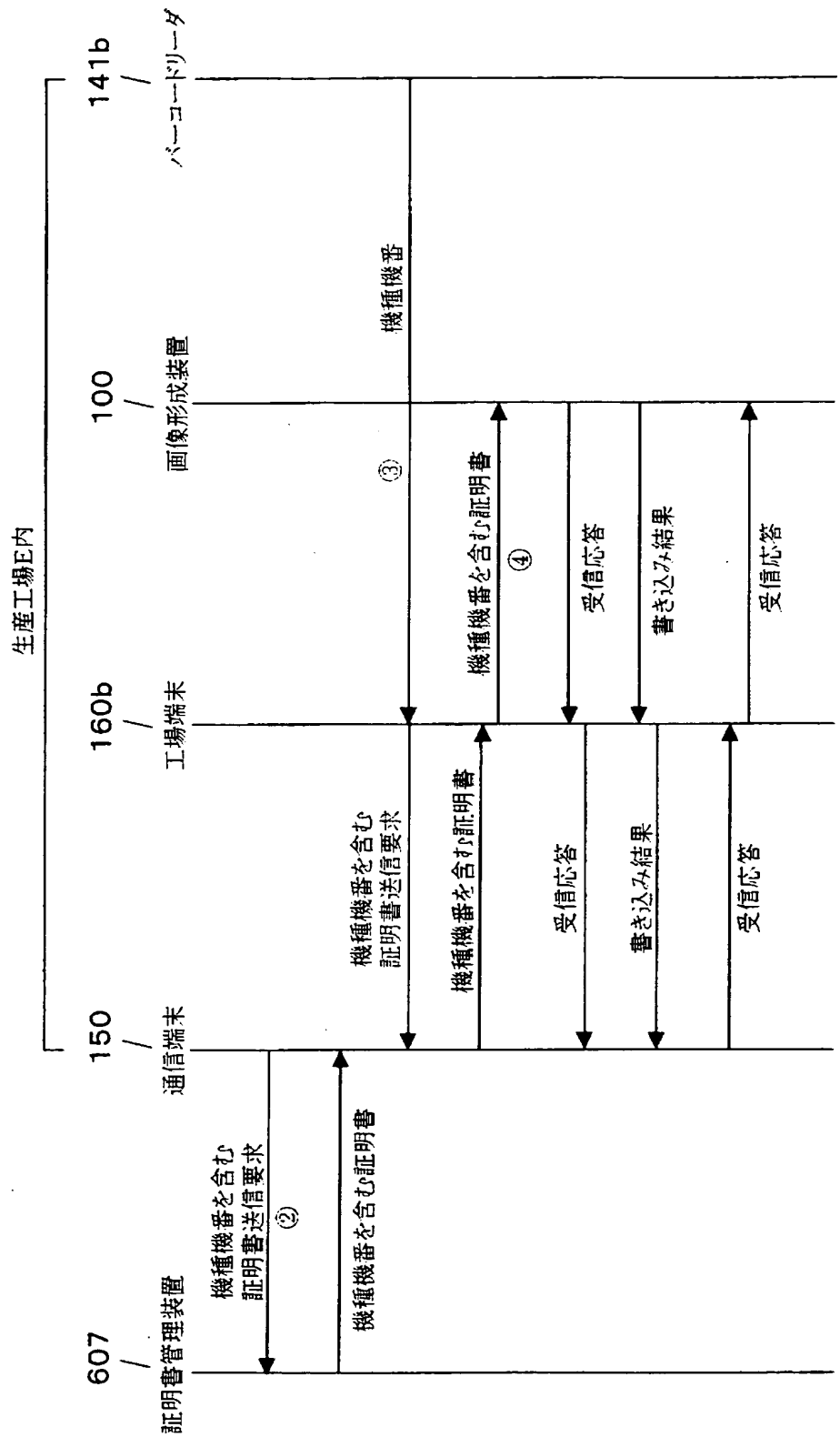
【図１６】


AICOO　画像形成装置　TYPE－1
定格電圧　定格消費電力　定格電流　機種コード
DC12V　3VA　0.25A　H100－00
機種機番
バーコード
BC

【図１７】


基板の組み立て
検査
共通証明書書き込み
工場端末
160
梱包
出荷
基板をカバーと合わせる
カバー関係の組み立て
製品機能の検査
証明書書き込みパラメータ初期化
工場端末
160
通信端末
150
外観検査
梱包
出荷

【図１８】


生産工場E内
607
証明書管理装置
150
通信端末
160b
工場端末
100
画像形成装置
141b
バーコードリーダ
機種機番を含む
証明書送信要求
②
機種機番を含む証明書
機種機番を含む
証明書送信要求
機種機番を含む証明書
受信応答
書き込み結果
受信応答
③
機種機番
機種機番を含む証明書
④
受信応答
書き込み結果
受信応答

【図１９】

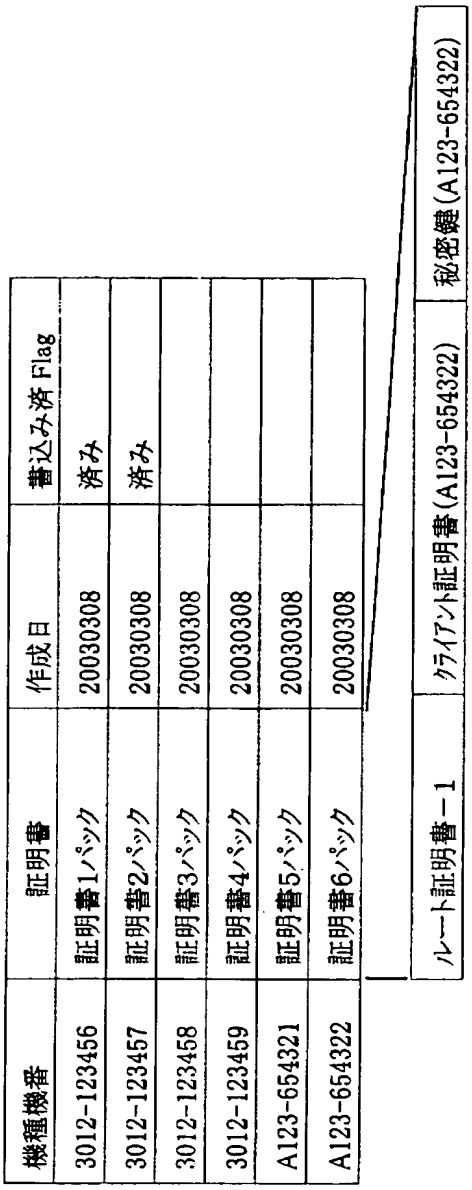
(a)

No	機種コード	証明書の有無	備考
1	3012	有り	
2	3013	なし	
3	3014	なし	
4	A123	有り	
5	A125	なし	

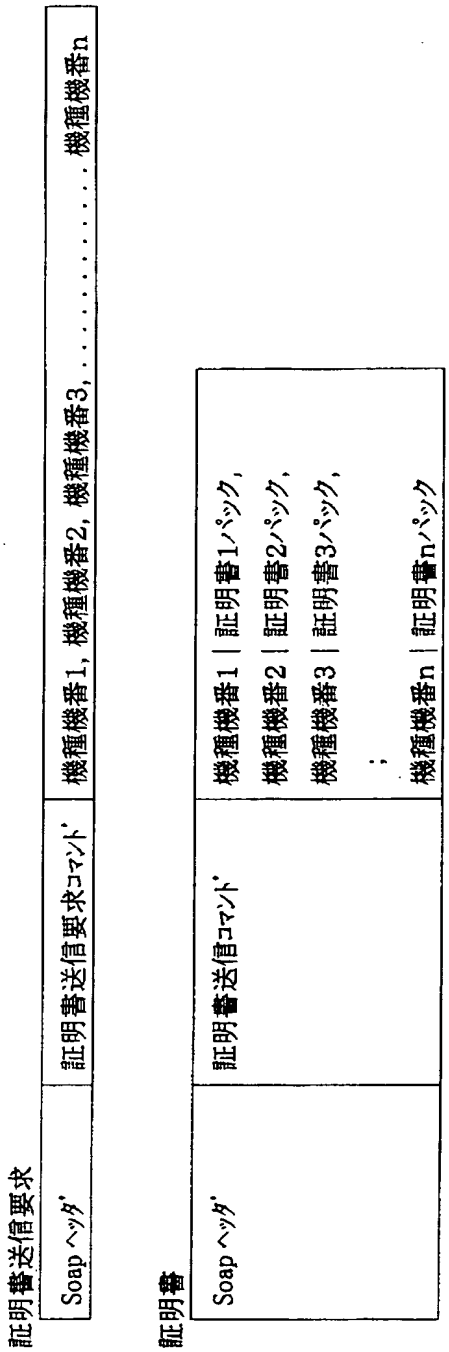
(b)

機種コード	3/17	3/18	3/19	3/20	3/24	3/25	3/26	3/27
3012	1000	1010	1020	1000	900	1200	1300	1100
3013	500	550	500	560	530	550	530	530
3014	560	570	560	560	540	570	550	550
A123	2120	2000	2130	2000	2000	2130	2110	2000
A125	2000	2001	2010	2020	2010	2000	2300	2000

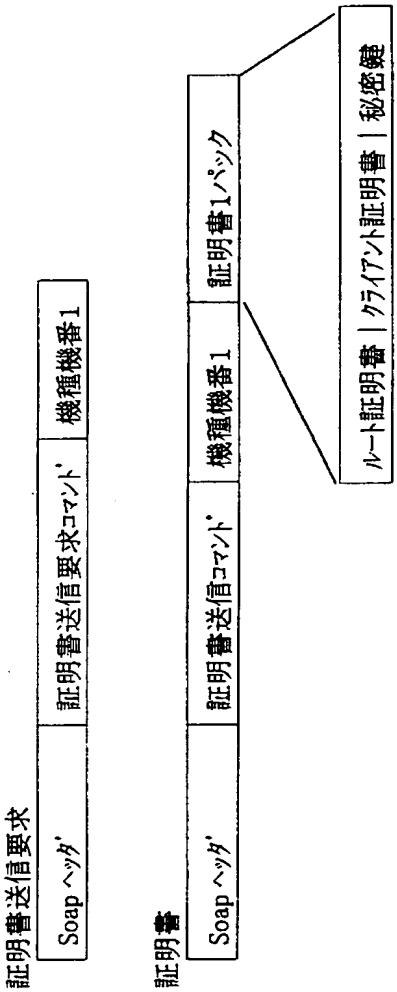
【図２０】


機種機番
証明書
作成日
書込み済 Flag
3012-123456
証明書1パック
20030308
済み
3012-123457
証明書2パック
20030308
済み
3012-123458
証明書3パック
20030308
3012-123459
証明書4パック
20030308
A123-654321
証明書5パック
20030308
A123-654322
証明書6パック
20030308
ルート証明書－1
クライアント証明書(A123-654322)
秘密鍵(A123-654322)

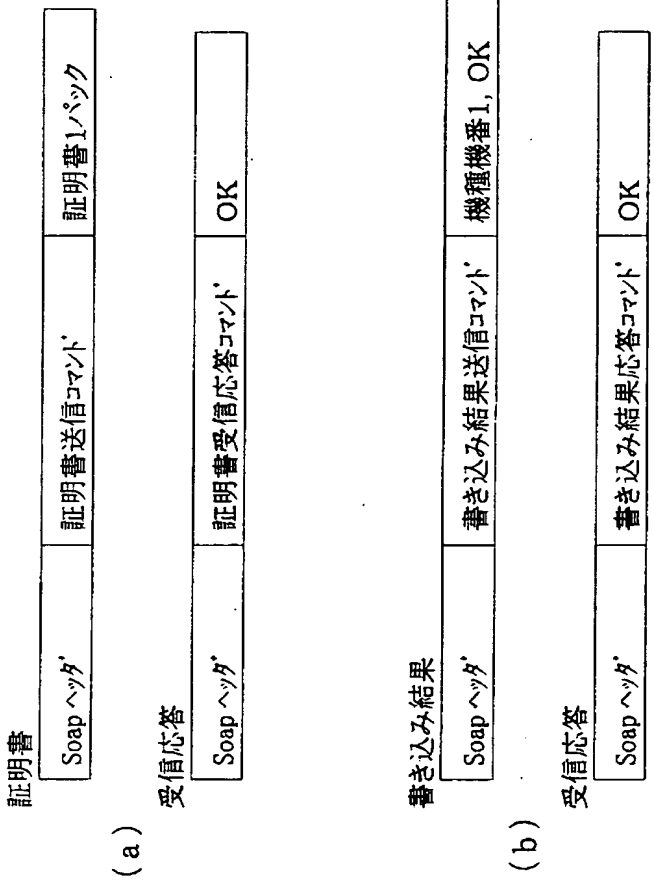
【図２１】


証明書送信要求
Soap ヘッダ'
証明書送信要求コマンド'
機種機番1, 機種機番2, 機種機番3, ... 機種機番n
証明書
Soap ヘッダ'
証明書送信コマンド'
機種機番1 | 証明書1パック,
機種機番2 | 証明書2パック,
機種機番3 | 証明書3パック,
;
機種機番n | 証明書nパック

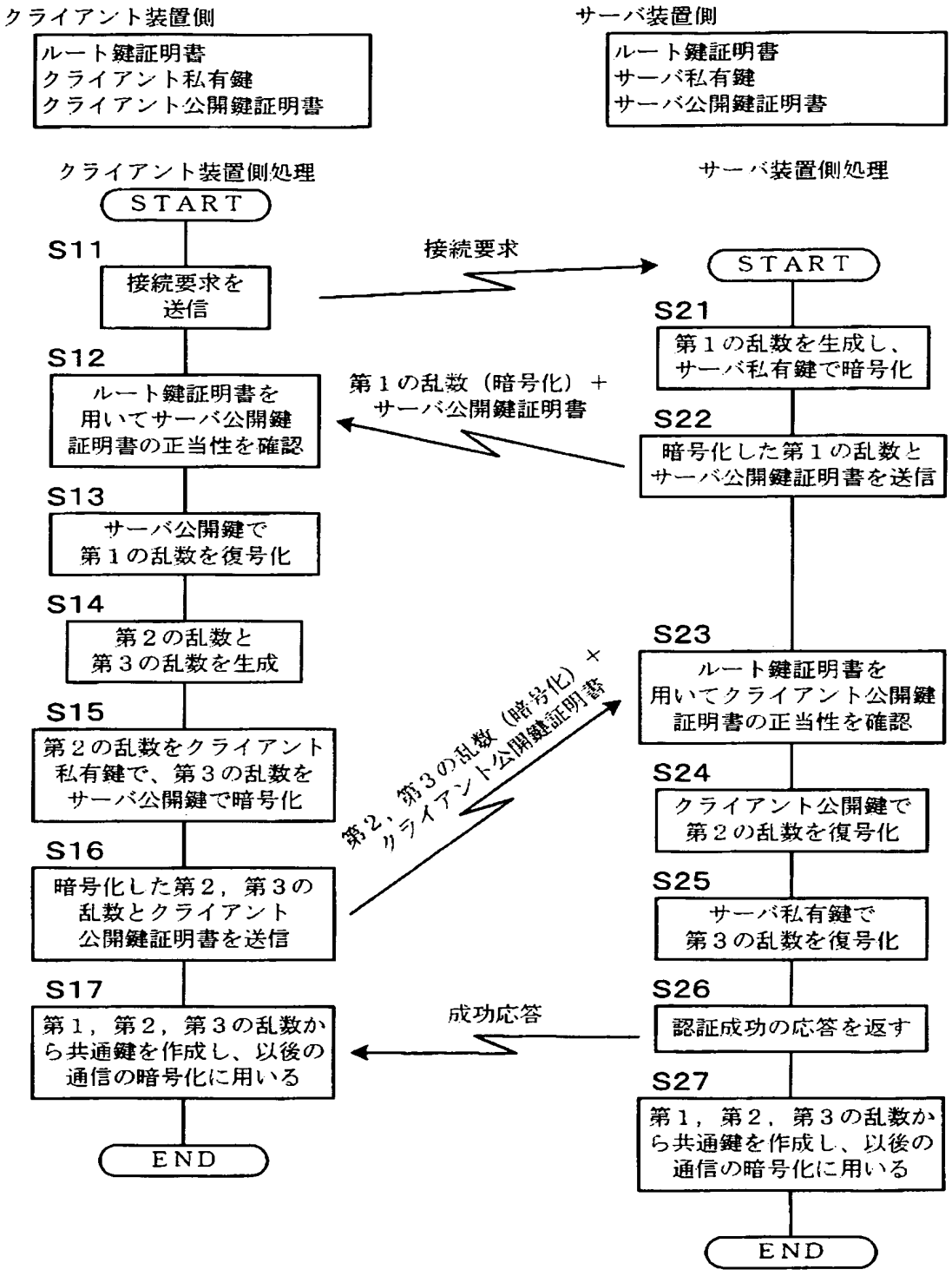
【図２２】


証明書送信要求
Soap ﾍｯﾀﾞ'
証明書送信要求ｺﾏﾝﾄﾞ'
機種機番1
証明書
Soap ﾍｯﾀﾞ'
証明書送信ｺﾏﾝﾄﾞ'
機種機番1
証明書1ﾊﾟｯｸ
ルート証明書｜クライアント証明書｜秘密鍵

【図２３】

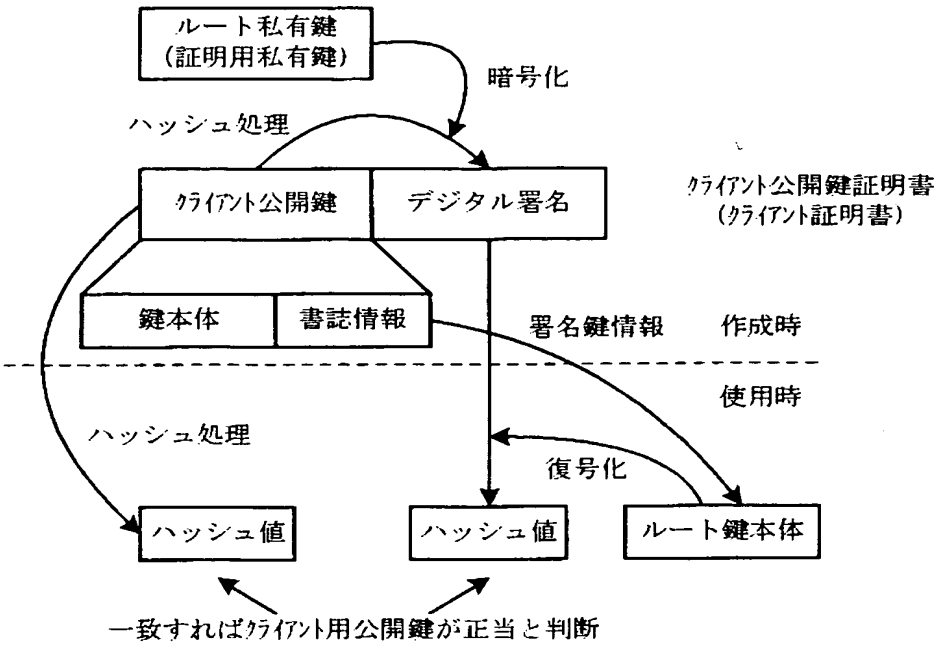

証明書
Soap ﾍｯﾀﾞ
証明書送信ｺﾏﾝﾄﾞ
証明書1ﾊﾟｯｸ
受信応答
Soap ﾍｯﾀﾞ
証明書受信応答ｺﾏﾝﾄﾞ
OK
(a)
書き込み結果
Soap ﾍｯﾀﾞ
書き込み結果送信ｺﾏﾝﾄﾞ
機種機番1, OK
受信応答
Soap ﾍｯﾀﾞ
書き込み結果応答ｺﾏﾝﾄﾞ
OK
(b)

【図２４】

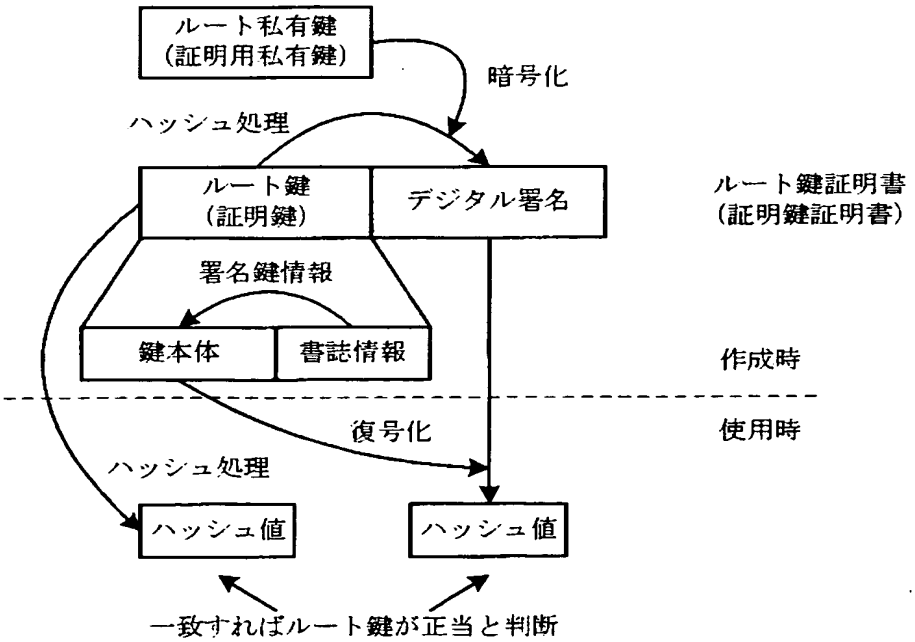

クライアント装置側
ルート鍵証明書
クライアント私有鍵
クライアント公開鍵証明書
サーバ装置側
ルート鍵証明書
サーバ私有鍵
サーバ公開鍵証明書
クライアント装置側処理
サーバ装置側処理
START
S11
接続要求を送信
接続要求
START
S21
第１の乱数を生成し、サーバ私有鍵で暗号化
S12
ルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認
第１の乱数（暗号化）＋サーバ公開鍵証明書
S22
暗号化した第１の乱数とサーバ公開鍵証明書を送信
S13
サーバ公開鍵で第１の乱数を復号化
S14
第２の乱数と第３の乱数を生成
S23
ルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認
S15
第２の乱数をクライアント私有鍵で、第３の乱数をサーバ公開鍵で暗号化
第２，第３の乱数（暗号化）＋クライアント公開鍵証明書
S24
クライアント公開鍵で第２の乱数を復号化
S16
暗号化した第２，第３の乱数とクライアント公開鍵証明書を送信
S25
サーバ私有鍵で第３の乱数を復号化
S17
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
成功応答
S26
認証成功の応答を返す
S27
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
END
END

【図２５】

（ａ）


ルート私有鍵
(証明用私有鍵)
暗号化
ハッシュ処理
ｸﾗｲｱﾝﾄ公開鍵
デジタル署名
ｸﾗｲｱﾝﾄ公開鍵証明書
(ｸﾗｲｱﾝﾄ証明書)
鍵本体
書誌情報
署名鍵情報
作成時
使用時
ハッシュ処理
復号化
ハッシュ値
ハッシュ値
ルート鍵本体
一致すればｸﾗｲｱﾝﾄ用公開鍵が正当と判断

（ｂ）


ルート私有鍵
(証明用私有鍵)
暗号化
ハッシュ処理
ルート鍵
(証明鍵)
デジタル署名
ルート鍵証明書
(証明鍵証明書)
署名鍵情報
鍵本体
書誌情報
作成時
使用時
復号化
ハッシュ処理
ハッシュ値
ハッシュ値
一致すればルート鍵が正当と判断

【書類名】　　要約書

【要約】

【課題】　中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定できるようにする。

【解決手段】　通信端末１５０のＣＰＵは、画像形成装置１００等の通信装置によるＳＳＬ通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番をその生産台数分だけ付加して証明書管理装置６０７へ通知し、その証明書管理装置６０７からその各機種機番をそれぞれ含む各証明書を受信すると、その各証明書を証明書ＤＢ１５４ａに保存した後、上記生産台数分の通信装置のいずれかの機種機番を示すバーコードがバーコードリーダ１４１で読み取られ、そのバーコードによる機種機番が工場端末１６０経由で入力されると、その機種機番に対応する証明書を証明書ＤＢ１５４ａから読み出して工場端末１６０により上記通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

【選択図】　　図１０

特願２００３－０９６２４０

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー